IPv4-IPv6 Transformer

User Manual

6/2013

V4.0.5

License

The End-User License Agreement (EULA) for the Datatek IPv4-IPv6 Transformer is detailed in Section 11 of the Datatek IPv4-IPv6 Transformer User Manual.

Printed in the USA.

Manufactured by:

Datatek Applications, Inc.
399 Campus Drive
Suite 140
Somerset, NJ 08873
Phone 732-667-1080
www.datatekcorp.com

TABLE OF CONTENTS

TABLE OF FIGURES

Important Safety Instructions

IMPORTANT SAFETY INSTRUCTIONS

The exclamation point within an equilateral triangle is intended to alert the user to the presence of important operating and maintenance (servicing) instructions in the literature accompanying the product.

When installing, operating, or maintaining this equipment, basic safety precautions should always be followed to reduce the risk of fire, electric shock, and injury to persons, including the following:

- Read and understand all instructions.
- Handle this product in conformity with the applicable building code.
- Follow all warnings and instructions marked on this product.
- For information on proper mounting instructions, consult the User's Manual provided with this product.
- Do not place this product on an unstable cart, stand or table. The product may fall, causing serious damage to the product.
- The Telecommunications interfaces should not leave the building premises unless connected to telecommunication devices providing primary and secondary protection, as applicable
- This product should be operated only from the type of power source indicated on the marking label. If you are not sure of the type of power supply, consult your dealer or local Power Company.
- Unplug this product from the wall outlet before cleaning. Do not use liquid cleaners or aerosol cleaners. Use a damp cloth for cleaning.
- Do not use this product near water, for example, in a wet basement.
- To reduce the risk of electrical shock, do not disassemble this product. Service should be performed by trained personnel only. Opening or removing covers and/or circuit boards may expose you to dangerous voltages or other risks. Incorrect re-assembly can cause electric shock when the unit is subsequently used.
- This product is equipped with a three-wire grounding type plug, a plug having a third (grounding) pin. This plug is intended to fit only into a grounding type power outlet. This is a safety feature. If you are unable to insert the plug into the outlet, contact your electrician to replace your obsolete outlet. Do not defeat the safety purpose of the grounding type plug. Do not use a 3-to-2-prong adapter at the receptacle. Use of this type adapter may result in risk of electrical shock and/or damage to this product.
- Do not allow anything to rest on the power cord. Do not locate this product where the cord will be abused by persons walking on it.
- Do not overload wall outlets and extension cords as this can result in the risk of fire or electric shock.

- Unplug this product from the wall outlet and refer servicing to qualified service personnel under the following conditions:
  a) When the powers supply cord or plug is damaged or frayed.
  b) If liquid has been spilled into the product.
  c) If the product has been exposed to rain or water.
  d) If the product does not operate normally by following the operating instructions. Adjust only those controls that are covered by the operating instructions because improper adjustment of other controls may result in damage and will often require extensive work by qualified technician to restore the product to normal operation.
  e) If the product has been dropped or the cabinet has been damaged.
  f) If the product exhibits a distinct change in performance.

SAVE THESE INSTRUCTIONS

Federal Communications Commission Statement

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio energy. If this equipment is not installed and used in accordance with the manufacturer's instructions, it may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment to an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

The circuit board is designed for installation in a shielded enclosure (metal or plastic with conductive coating). Shielded cables are required on LAN and serial ports to assure compliance with FCC regulations.

A copy of the test report will be provided on request.

1 FAQ

Here are answers to some of your most frequently asked questions:

Q1. ***What's an IPv4-IPv6 Transformer?***

A1. The Datatek Applications IPv4-IPv6 Transformer changes a legacy IPv4-only device into a dual-stack IPv4/IPv6 host.

Q2. ***What's a legacy IPv4-only device?***

A2. It could be a PC, a server, a printer, a network appliance - it's anything with a LAN port that doesn't understand the new Internet Protocol Version 6, or IPv6. Virtually every device with a LAN port understands Internet Protocol Version 4, or IPv4. Since the inception of the Internet, IPv4 has become so ubiquitous that no one bothered to mention the version number and simply referred to it as IP, or TCP/IP. One day IPv6 will completely replace IPv4. (Some people think that the sun will burn out before this happens.) In the mean time, IPv6 and IPv4 will coexist and new devices will support both protocols. Legacy devices that only support IPv4 will be at disadvantage.

Q3. ***How do I connect to your Transformer?***

A3. It's simple. The Transformer has two LAN ports, a host-side port and a network-side port. First, disconnect your legacy device from the network and plug it into the Transformer's host-side port. Next, hook the Transformer's network-side port up to your network. Finally, configure the Transformer using a web-browser and you're done.

Q4. ***Do I have to install your software on my legacy device?***

A4. No, there's no software to install on the legacy device.

Q5. ***Will I need to make any changes to my legacy device?***

A5. Typically, you will need to change the legacy device's IPv4 address, subnet mask, default router and DNS server. This is because the Transformer uses the legacy device's original IPv4 address on its network-side port, and the legacy device will use a private address that's only visible on the host-side of the Transformer. However, if the legacy device is set up to get these parameters from a DHCP server, the Transformer will automatically reconfigure the legacy device.

Q6. ***How hard is it to configure the Transformer?***

A6. The Transformer is shipped with a default configuration that provides basic capabilities for a typical device. If this default configuration works for you, no changes are required. For more complex features and special network configuration, the Transformer provides a secure, web-based graphical user interface (GUI) that's accessible from either the host or network side ports, using either IPv4 or IPv6. In addition, a serial console interface enables initial configuration when the LAN ports are unavailable.

Q7. ***Why shouldn't I just upgrade the software on my legacy device to support IPv6?***

A7. If you can, you should. However, this may be more difficult than it appears. The software running on a legacy device typically consists of an operating system and several network applications. Both the operating system and the network applications will need to be upgraded to support IPv6. For older systems, upgrades for every component may not be available. Even when upgrades are available, the cost of the new software and additional costs to re-test and re-certify it may be prohibitive. In these cases, the Transformer is a cost-effective solution.

Q8. ***How many legacy devices can a Transformer support?***

A8. The Transformer has a feature called Local Forwarding, which is used to add extra IPv4 host nodes with IPv4-IPv6 packet translation. This functionality is directed by 'forward mapping'. Without any forward mappings, the Transformer acts as a full IPv6 surrogate for one IPv4 host. With forward mapping enabled, the Transformer can perform address and protocol translation for additional IPv4 endpoints on the host-side network. However, the Transformer cannot act as a full IPv6 surrogate for those other IPv4 endpoints.

Q9. ***If I use a Transformer, can my legacy device still use IPv4 to communicate with other legacy devices on the network that don't have Transformers?***

A9. Yes. The Transformer adds IPv6 capability to a legacy device that only supports IPv4. It doesn't remove the legacy device's IPv4 capability or connectivity.

Q10. ***Can I put a Transformer between two routers?***

A10. No, that's not supported.

Q11. ***My legacy device gets its IP address from a DHCP server. Will this still work with a Transformer?***

A11. Yes, the Transformer can act as a DHCP server to the legacy device.

Q12. ***My legacy device connects to hosts by using domain names, not IP addresses. Can it still do this?***

A12. The Transformer has a DNS ALG (Application Layer Gateway) that will forward your legacy device's queries for an IPv4 address to a DNS server. The DNS ALG will prefer finding an IPv6 address for a DNS query and will return a proxy IPv4 address to the host.

Q13. ***Does the Transformer provide any security?***

A13. Yes, IPsecv2 and IPsecv3 are both supported, along with a choice of several cryptographic algorithms. The Transformer acts as an IPsec proxy for your IPv4 legacy device. The secured path will be between the Transformer and a remote host that also supports IPsec. The path between your legacy device and Transformer is not secured, but since they are supposed to be co-located and tightly coupled, this should not be a problem.

Q14. ***Has the Transformer been certified by an independent 3rd party?***

A14. The Transformer has passed the IPv6 Ready Phase-2 Gold Core, USGv6 Basic, SLAAC, Address Architecture and IPsec Conformance tests as performed by the University of New Hampshire (UNH) interoperabilty test lab. The Transformer has been certified for IPv6 by the Joint Interoperability Test Command (JITC), which is the official DoD test agency.

Q15. ***The status bar at the bottom of my web browser shows "Waiting for [address]".***

A15. Some web browsers such as Mozilla Firefox may show "Waiting for [address]" in the status bar at the bottom instead of "Done" after the page is loaded. This can be ignored.

Q16. ***I logged into the GUI and when I opened another connection, I was not re-prompted to log in.***

A16. The login and password dialog box for the Transformer's web browser GUI may not appear for subsequent connections from a browser session that has previously established a login to the Transformer's GUI.

Q17. ***Why doesn't the Transformer's webGUI have a logout button?***

A17. The Transformer uses HTTP authentication. For every page you request from the Transformer, your browser sends the username and password from its cache. There is no reliable way to force the browser to "forget" the username and password, and session management to work around that would introduce potential security vulnerabilities, so the Transformer does not provide a log out functionality. To safely log out, close your browser.

Your web browser may have a way to clear cached HTTP credentials. Check your browser's documentation for further information.

2 Overview

Throughout this document, the following definitions and conventions will be used:
Host-side refers to the attachment point for the IPv4 legacy device. This is the physical connection labeled IPv4 on the Transformer's front panel. *Network-side* refers to the IPv6 or IPv4/IPv6 dual network which is connected to a hub or router. This is the physical connection labeled IPv6 on the Transformer's front panel.

2.1 How the Transformer Works

The Transformer has two interfaces, the host-side and network-side interfaces. The legacy IPv4 device is connected to the Transformer on the host-side IPv4 interface while the IPv6 network is connected on the network-side IPv6 interface. The Transformer receives IPv4 packets from the legacy IPv4 device through the IPv4 interface and translates them into IPv6 packets to send out the network-side interface. It receives IPv6 packets from the network-side interface and translates them into IPv4 packets and sends them out the host-side interface. The Transformer uses a mapping table that contains one-to-one bindings between surrogate IPv4 addresses and IPv6 addresses. The binding between the legacy IPv4 address and its proxy IPv6 address is automatic. Other bindings are either configured manually using the Static address map form or created dynamically by the Transformer when it selects an available IPv4 address from the IPv4 address pool that was configured on the Address pool form.

The Transformer has IPv4 and IPv6 addresses assigned to represent itself to the world for management purposes, but the Transformer also establishes *public* IPv4 and IPv6 addresses to represent the host's *private* IPv4 address.

When the IPv4 host sends a packet to an IPv4 address on the network side, the Transformer substitutes the host's private IPv4 address with the public IPv4 address representing the host on the Transformer, and then transmits that packet to the network. When the IPv4 host transmits a packet to an IPv6 endpoint, its private IPv4 address is mapped to the public IPv6 address on the Transformer, the surrogate destination IPv4 address is mapped to the actual IPv6 destination, and protocol translation from IPv4 to IPv6 is performed. This packet is then routed to the network IPv6 address.

If the IPv4 host looks up the IP endpoint by name, the Transformer handles the DNS request, forwarding it to the network's DNS when necessary. If the network's DNS returns an AAAA record, meaning there is an associated IPv6 address for that name, the Transformer will choose a surrogate IPv4 address from the address pool and set up a binding for that surrogate IPv4 to the IPv6 address returned from DNS. The Transformer then passes the surrogate IPv4 address as the response to the host's DNS request. If the DNS returns only an A record, that IPv4 address is transmitted as the answer to the host's request.

Packets arriving from the network are translated in a complementary fashion. When a packet arrives at the Transformer for the host's public IPv4 address, the Transformer replaces that address with the host's private address and forwards the packet to the host. When an arriving packet is addressed to one of the host's IPv6 public addresses, the Transformer looks up the IPv6 source address in the binding tables. If the address is not found, a new binding is created using an available IPv4 address from the pool. The source and destination addresses are then translated to the corresponding IPv4 addresses while the packet is converted from IPv6 to IPv4.

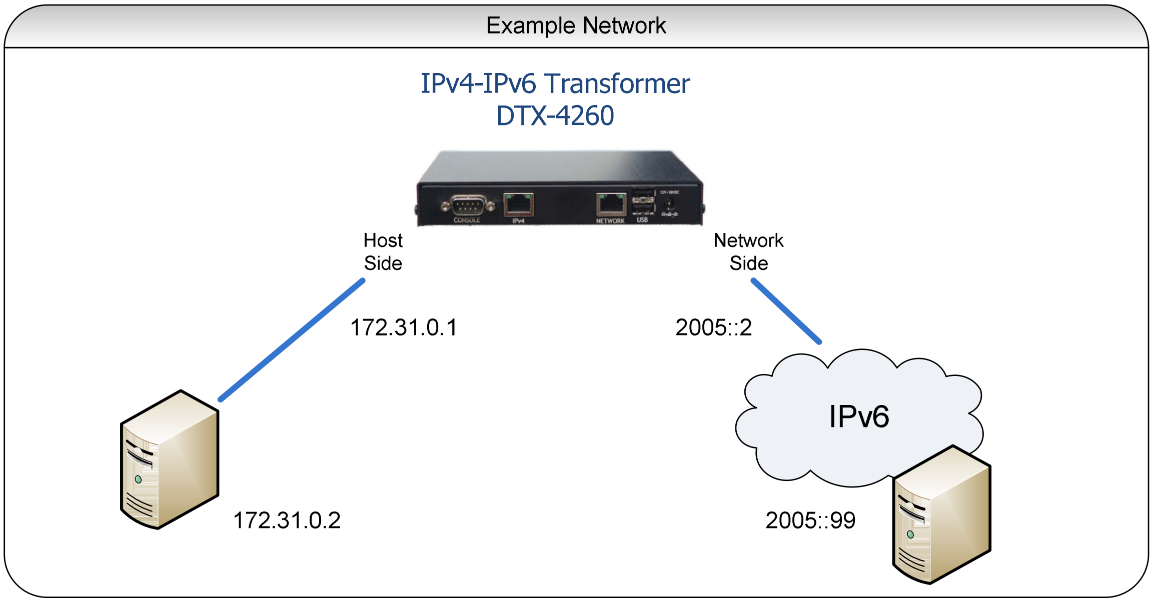


Figure 1. Overview IP Addresses

Figure 1. Overview IP Addresses displays the actual IPv4 and IPv6 addresses of each network device in our example network.

After the Transformer has been configured, the IPv4 host and IPv6 devices will have two different perspectives, as shown in **Figure 2. Host Perspective** and **Figure 3. Device Perspective**

From the IPv4 host's perspective, as shown in **Figure 2. Host Perspective,** all IPv6 addresses on the IPv6 network appear to be using IPv4 addresses. From the IPv6 devices' perspective, as shown in **Figure 3. Device Perspective,** all IPv4 addresses on the IPv4 host side appear to be using IPv6 addresses.

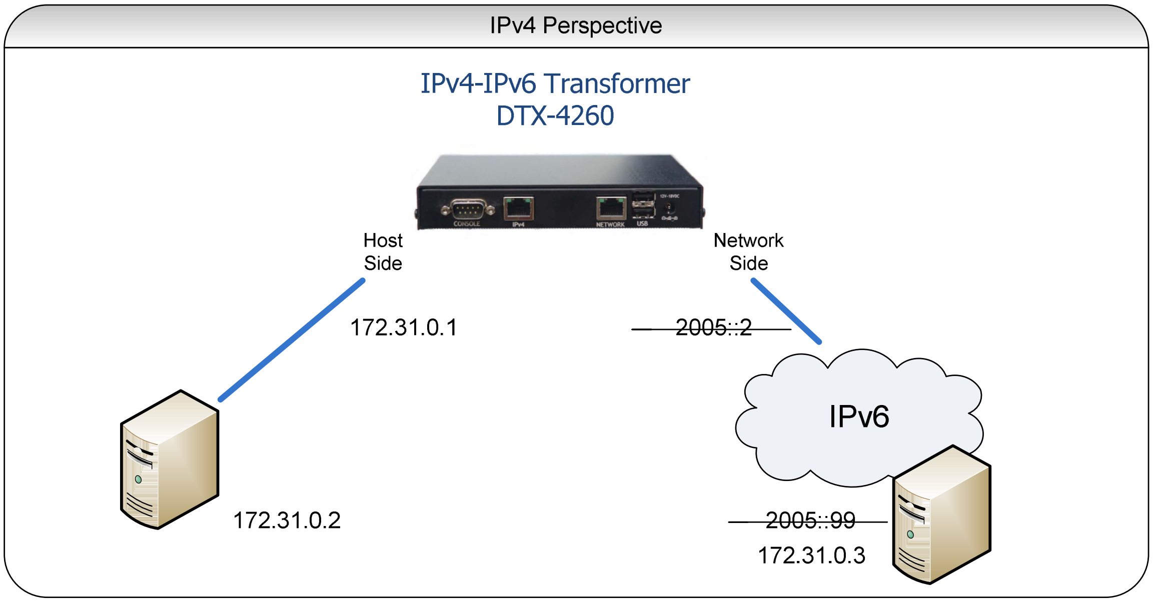


Figure 2. Host Perspective

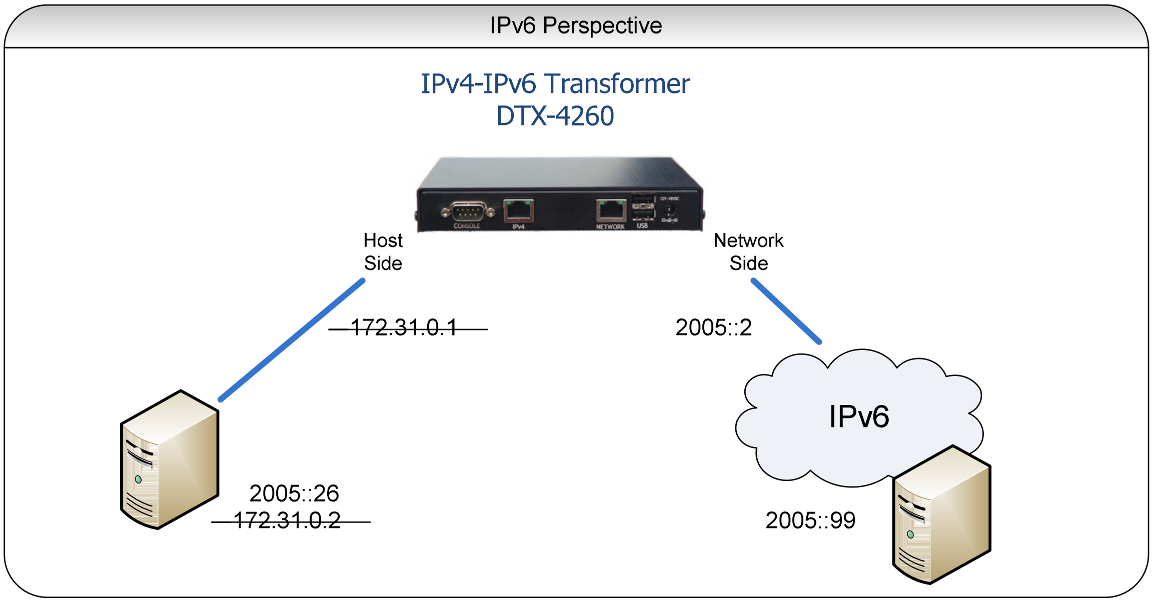


Figure 3. Device Perspective

The Transformer has a feature called Local Forwarding, which is used to add extra IPv4 host nodes with IPv4-IPv6 packet translation. This functionality is directed by 'forward mapping'. Without any forward mappings, the Transformer acts as a full IPv6 surrogate for one IPv4 host. With forward mapping enabled, the Transformer can perform address and protocol translation for additional IPv4 endpoints on the host-side network. However, the Transformer cannot act as a full IPv6 surrogate for those other IPv4 endpoints.

The mappings added for forwarding are different from the primary address bindings. The primary bindings (static, DNS and ingress) map existing IPv6 addresses into surrogate IPv4 addresses, seen only on the host-side network, that allow host-side endpoints to reach the IPv6 world using IPv4 addresses. Bindings for forwarding map existing IPv4 addresses on the host side into surrogate IPv6 addresses that network-side endpoints can use to reach endpoints on the host side through the Transformer.

The extra surrogate IPv6 addresses allow the Transformer to perform packet translation between IPv4 endpoints on the host side (other than the host itself) and IPv6 endpoints on the network side. However, they do not provide full Transformer functionality for those endpoints. For example:

- The DHCP6 client cannot obtain IPv6 addresses for these endpoints
- The Transformer cannot auto-configure any IPv6 addresses, e.g. link local for these endpoints
- There is only one IPv6 address assigned to each IPv4 address, and therefore only one IPv6 scope for any endpoint set up this way
- IPv4 passthrough cannot be done to these extra hosts

Using forward mapping and static routes, the IPv4 address space on the host side can be more elaborate than just a simple host subnetwork. For example:

- The host or some other endpoint on the host side can provide forwarding; the Transformer can be configured with an appropriate static route. This may allow IPv4 passthrough
- The surrogate IPv6 addresses used in forward mapping can belong to an IPv6 subnetwork different from the Transformer; a router on the IPv6 network side can be configured to forward those addresses through the Transformer.

Complications can easily cause serious problems. For example:

- A DHCP server on the host side can interfere with the Transformer
- Any endpoint on the host subnetwork that is *not* in the local forwarding list will have an **arp** conflict with the Transformer
- IPv4 connectivity of any equipment on the host side that might reach the main network (on the Transformer's IPv6 side) without going through the Transformer might cause problems

Figure 4. Local Forwarding, shows a primary IPv4 device and other secondary IPv4 endpoints behind the Transformer.

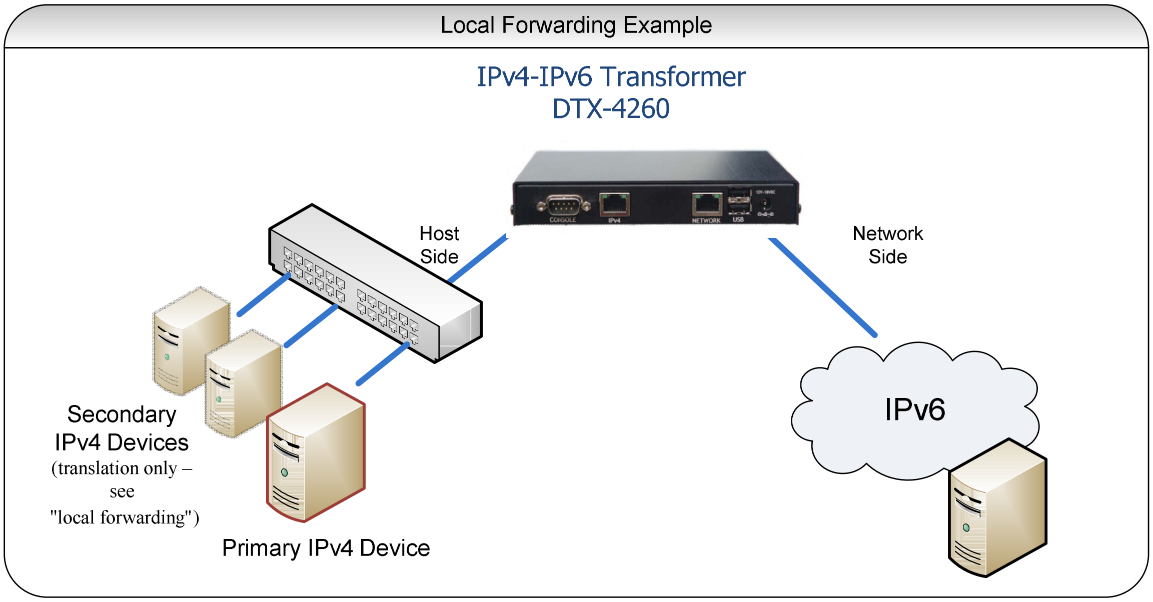


Figure 4. Local Forwarding

2.2 Key Features

Autoconfiguration

The Transformer supports the Stateless Address Autoconfiguration (SLAAC) protocol described in RFC2462, and an extension to SLAAC for supporting temporary addresses as described in RFC3041 in configuring the network-side IPv6 address interface.

The Stateless Address Autoconfiguration (SLAAC) process employs the Neighbor Discovery Protocol (NDP) which includes Router Solicitations/Advertisements and Neighbor Solicitation/Advertisements. The NDP messages are used to verify that the link local address is unique on the link. The Router messages are used to discover the network prefix of the Transformer's IPv6 link. The prefix is combined with the interface identifier of the link local address to create a global IPv6 interface address. This address is then configured as the Transformer's IPv6/Network interface's IPv6 address. A proxy IPv6 address is also autoconfigured for the IPv4 legacy device by using the host-side interface's MAC address as the interface identifier for the proxy IPv6 address. The proxy IPv6 address is then bound to the IPv4 address of the legacy device.

The SLAAC process independently supports both the Transformer as an endpoint and the host as a proxy endpoint.

When temporary addresses are enabled on the Transformer, the interface identifier is a randomized value that is regenerated periodically and combined with the network prefix that was advertised in the router advertisements to create a temporary address that is difficult to eavesdrop due to its changing nature

DNS Server

The Transformer uses a DNS Application Layer Gateway (ALG) to act as a proxy DNS Server for the IPv4 legacy device. As a proxy, the Transformer processes DNS lookups and reverse lookups sent from the legacy device. A DNS lookup requests the IP address for a given domain name. A DNS reverse lookup requests the domain name for a given IP address. Henceforth, an *A-record* query will refer to a DNS lookup of an IPv4 address for a given domain name and an *AAAA-record* query will refer to a lookup for an IPv6 address for a given domain name.

DNS Lookup or A/AAAA-record Query

The Transformer receives A-record queries from the IPv4 legacy device and translates them into AAAA-record queries before forwarding them to the network's DNS Server. The DNS Server either responds with an IPv6 address or not. If an IPv6 address is received in response, the IPv6 address is mapped to an available IPv4 address from the IPv4 Address pool. The AAAA-record response is then translated into an A-record response containing the IPv4 address and forwarded to the legacy device. To the IPv4 legacy device, the IPv4 address looks as if it came from the DNS Server directly.

If the network's DNS Server does not respond to the AAAA-record query, the Transformer tries to get an IPv4 address for the domain name by sending the DNS Server an A-record query. The A-record response is then forwarded to the IPv4 legacy device without translation.

Reverse DNS Lookup or PTR-record Query

The DNS ALG also supports reverse lookups. Henceforth, Pointer (PTR) record will refer to reverse lookups that ask for the host and domain name of a given IP address. If the Transformer receives a PTR-record query for a given IPv4 address, it checks if it is mapped to an IPv6 address. A mapping may exist if an IPv6 host on the network initiated a session with the IPv4 legacy host and the packet received from the network contained the IPv6 address of the remote IPv6 host as the source address. This IPv6 source address would have been bound to an available IPv4 address from the Address pool before the packet was forwarded to the legacy device. The legacy device could then send a PTR-record query for the IPv4 address from the address pool. In this case the Transformer must translate the IPv4 PTR-record query into an IPv6 PTR-record query for the domain name of the IPv6 address to which the IPv4 address is mapped. The IPv6 PTR-record query is sent to the DNS Server. The IPv6 PTR-record response from the DNS Server contains a domain name that is then translated into an IPv4 response containing the same domain name unchanged.

It is also possible for the Transformer to receive a PTR-record query for an IPv4 address that is not bound to an IPv6 address. In the case of Passthrough, which is used for communication between two IPv4 hosts, there is no IPv4/IPv6 binding. The Transformer forwards a PTR-record query from the legacy device for an unbound IPv4 address directly to the DNS Server. The response is forwarded directly to the legacy device.

Configuration

The DNS Server address for the IPv6 network is either manually configured on the General Setup form or may be served from a DHCPv6 Server as specified on the DHCPv6 client form.

DHCPv6 Client

The Transformer can be configured on the DHCPv6 client screen to act as a DHCPv6 client to receive an IPv6 address for itself along with other host configuration parameters from a DHCPv6 server. The Transformer can also receive the IPv6 proxy address for the host.

DHCPv4 Server

The Transformer can be configured on the DHCPv4 server screen to act as a DHCPv4 server to the IPv4 legacy device to provide the IPv4 legacy device with an IP address and other host configurations. The IPv4 address that is served to the IPv4 legacy device is the IPv4 address that was configured on the Interface Setup screen. This DHCP feature satisfies those IPv4 devices that do not store their own IPv4 addresses but require a DHCP Server to give one to them.

Passthrough

The legacy IPv4 device can talk to other IPv4 devices across the network. In pass-through, the Transformer does not translate IPv4 packets, but maps the IPv4 address representing the host. In the direction from the IPv4 legacy device towards the network, the legacy device only needs to ensure its routing table contains an entry for the subnet or host address of the IPv4 destination host and that the gateway or next hop for that subnet or host address is the Transformer's host-side interface address as configured on the Interface Setup screen's host-side **Transformer IPv4 address**. IPv4 hosts on the network can talk to the legacy host by addressing the legacy host with the **Device IPv4 Address** that was configured in the network-side section of the Interface Setup screen.

This feature may be useful for situations where not all the IPv4 devices on a link can be moved behind Transformers at one time. The devices then must be separated by placing some of the IPv4 devices on the network-side of the Transformer and a single IPv4 device behind the Transformer on the host-side. Pass-through is then used to enable communication between the IPv4 device on the host-side and all the other IPv4 devices on the network-side.

Address Pool

The transformer configuration includes a range, or multiple ranges, of IPv4 addresses that it can use to satisfy the need to map network-side IPv6 addresses to host-side IPv4 addresses. The processes described above, in which new IPv6 addresses are added to the list of endpoints reachable by the legacy host, requires a supply of IPv4 addresses available to combine, one-to-one, in bindings of IPv6 addresses to IPv4 addresses. This supply is called the **address pool**.

The designated private IPv4 address ranges are the best choice to be used to supply the pool. But it is required that IPv4 addresses in the address pool must be addresses that are not reachable on the network side.

Address Resolution

In the normal course of sending and receiving packets with IPv6 endpoints, the legacy host is working only with IPv4 addresses, most likely with addresses that have come from the pool. These IPv4 addresses may or may not be in the same subnetwork as the host. Addresses within the subnetwork are reached after a suitable ARP exchange, while addresses not in the same subnetwork should be directed toward the host interface of the transformer by means of a static or gateway route. The gateway is configured either manually on the legacy host or automatically if the host is configured for DHCP. When ARP is initiated by the host, the transformer replies with its own interface address. In these two ways, all IPv4 traffic to the surrogate IPv4 addresses travels through the transformer's host-side interface.

Local Forwarding

Local forwarding allows expanding the Transformer to work with more than one legacy host, as discussed above. There are some caveats, however, to their use that must be mentioned. The locally forwarded endpoints do not support SLAAC, nor do they support the IPv4 pass-through mode. The locally forwarded endpoints can receive addresses from the DHCPv4 server, as will be detailed in a later section. None of these DHCP leases will appear on the DHCP leases screen, however. In addition, Diagnostics will not function properly for these endpoints.

Internet Protocol Security (IPsec)

The Transformer can be configured to provide IPsec protection on behalf of an IPv4 legacy device and locally forwarded IPv4 endpoints. The secured path lies between the Transformer and the remote host. Specifically, IPsec is terminated at the IPv6 endpoints; the IPv6 address that represents the IPv4 legacy device and the IPv6 address of the remote host. Since the path between the legacy host and the Transformer is not secured, they should be co-located in a secured area.

To enable IPsec, the administrator must configure the Security Policy (SP) and may manually configure a Security Association (SA). The SP specifies the packets that should be protected by describing the characteristics on which to match a user packet; e.g. the IP address and port number, and the upper layer protocol. The SA specifies how they should be protected; e.g. the algorithms and keys to use.

3 Physical Setup

3.1 Transformer Physical Description

The Transformer's rear and front views are shown below in **Figure 5. Transformer Rear View** and **Figure 6. Transformer Front View.**

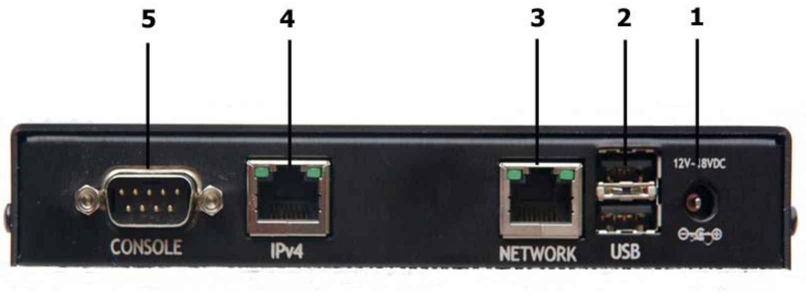


Figure 5. Transformer Rear View

	Feature	Description
1	Power Input	12-18VDC center positive power adapter
2	USB	USB ports – not used at this time
3	Network (IPv6 Port)	LAN port supports 10-BASE-T or 100-BASE-T
4	IPv4 Port	LAN port supports 10-BASE-T or 100-BASE-T
5	Serial Console	9 pin serial console interface

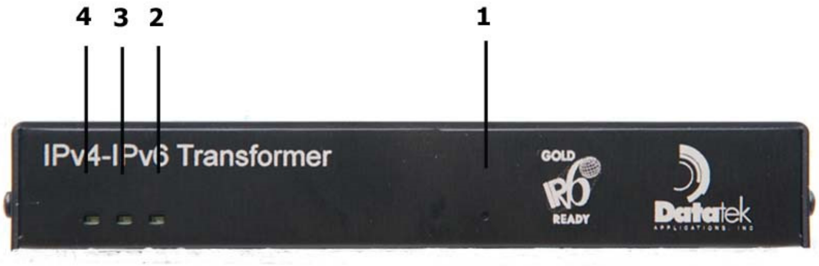


Figure 6. Transformer Front View

	Feature	Description
1	Reset Button	Button used to reboot the unit
2	LED	Lights while booting
3	LED	Lights while booting
4	LED	Power

3.2 Transformer Setup

The Transformer must be set up and minimally configured in order to use a web browser to completely configure the Transformer. To setup the Transformer:

Unpack the Transformer and its power cable.

Connect the Transformer's IPv4 port to the IPv4 device with standard Ethernet cables, for example, Cat 5.

Connect the Transformer's IPv6 Network port to the IPv6 network with standard Ethernet cables, for example, Cat 5.

Connect the console port to an ASCII terminal, PC com port (with terminal emulator) or via a console access device. Terminal settings are: 9600 baud, 8 bit, no parity, one (1) stop bit (8N1). The console cable used should be a cross-over (db9 pin, null-modem) cable. See Appendix A for the crossover connector pinout diagram.

Note

The console port is used for initial configuration of the Transformer. It's possible to do the initial configuration using the IPv4 port, provided that the factory default IP address assigned to the port works for you.

Power up the Transformer, and monitor booting from the console. You may safely ignore traces during the boot process.

The following is what the user will typically see during the boot process:

```
/kernel text=0x4c70d8 data=0x50714+0x5b47c \-----------------------
Loading mfsroot...6000000 0107 0280 00 00 00 00000000 00000000
Booting...B 0020 02000000 0107 0290 00 3F 00 0000E101 A0000000 10
.
.
.
Trying to mount root from ufs:/dev/md0a
Found configuration on ad0.
Initializing timezone... done
Initializing PC cards... failed (probably no PC card controller present)
Configuring firewall... done
Configuring LAN interface... done
Configuring WAN interface... done
Starting syslog sservice... is1: link state changed to DOWN
done
Starting webGUI... done
Starting DNS forwarder... done
Starting DHCP service... done
Starting NTP client... done
Initializing SSH...started sshd
```

```
Setting proxy link-local address ...done
Configuring address pool...done
Configuring IPsec ... done


*** Datatek IPv4-IPv6 Transformer Version 4.0.0
   Disk 093010.2 made by v6adm
   Build 093010.1 made by v6adm
   Copyright (C) 2010 Datatek Applications Inc. All rights reserved.
   Code imported from m0n0wall:
   Copyright (C) 2002-2005 by Manuel Kasper. All rights reserved.

   Initial GUI IP address: 172.31.0.1

   Port configuration:

   LAN   -> sis1
   WAN   -> sis0

FreeBSD/i386 (skf.local) (console)
```

If the console messages do not look like the messages above, but instead look like the following, then make sure the Compact Flash is plugged in all the way.

```
0:19:0 0E11 A0F8 0C031008 0117 0280 08 38 00 A0003000 00000000 11

 1 Seconds to automatic boot.   Press Ctrl-P for entering Monitor.

NSC DP83815/DP83816 Fast Ethernet UNDI, v1.03
Copyright (C) 2002, 2003 National Semiconductor Corporation
All rights reserved.

Pre-boot eXecution Environment  PXE-2.0 (build 082)
Copyright (C) 1997-2000  Intel Corporation


CLIENT MAC ADDR: 00 00 24 C4 F9 4C
PXE-E53: No boot filename received


PXE-M0F: Exiting MacPhyter PXE ROM.

No Boot device available, enter monitor.


comBIOS Monitor.   Press ? for help.

> R
```

After booting, you will be greeted with the **login** prompt, as shown below. You can enter any character at this time, which will bring you to the Console Main Menu, as shown below.

However, if the Console Main Menu does not appear on the console within about 3 minutes of booting, contact support. More information on the Console Main Menu configuration selections is discussed in the next section.

```
login: test


Datatek Transformer Console
**********************
1) Set up IPv4 and IPv6 interfaces
2) Reset webGUI password
3) Reset to factory defaults
4) Reboot system
5) Ping host
6) Change password
7) Logoff

Enter a number:
```

When the Transformer is shipped from the factory, the host-side IPv4 address is set to 172.31.0.1. The network-side port is not assigned an IPv4 address. However, network-side port has an IPv6 link-local address and it will participate in IPv6 Stateless Address Autoconfiguration.

4 Console Interface

The console port lets you access the console interface to the Transformer. You must use the console interface when you first install the Transformer to assign IP addresses to the host and/or network side ports. You only need to use the console interface when you can't reach the webGUI through either the host or network side LAN ports. You may also need to use the console interface if you make a serious mistake when configuring the Transformer with the webGUI, like changing the password to something you immediately forget. Configuring and accessing the webGUI is discussed in the next section.

To use the console interface, you must connect the console port to an ASCII terminal, a PC com port (with terminal emulator) or via a console access device. Terminal settings are 9600 baud, no parity, one (1) stop bit. The console cable used should be a cross-over (9 pin, null-modem) cable. See Appendix B for the crossover connector pinout diagram.

While booting, the Transformer prints a large amounts of information on the console that is mainly of interest to the software developers. However, the console interface is active during this period and it is possible to pause or modify the boot process by entering commands. These commands are for development and testing use only and are not documented in this manual.

After booting, you will be greeted with a login prompt. As shown in the example below, you must use the login id **root**. Once you enter the login id, it will prompt you to enter a password. From the factory, the default password is the Enter key. Later on, you may change the password to one of your own choosing. The Transformer prints the Console Main Menu, and prompts you to enter a number corresponding to a menu item. Each of these menu items are described in more detail in Section 6.

```
login: root


Datatek Transformer Console
**********************
1) Set up IPv4 and IPv6 interfaces
2) Reset webGUI password
3) Reset to factory defaults
4) Reboot system
5) Ping host
6) Change password
7) Logoff

Enter a number: 1
```

5 WebGUI Interface

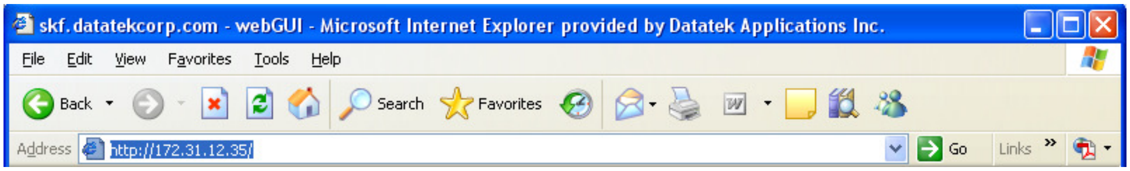
The Transformer provides a web server to support configuration and management through any standard web browser such as MS Internet Explorer, Mozilla Firefox, etc. The webGUI can be accessed from either the IPv4/Host or the IPv6/Network interfaces.

1. Start a web browser.

2. In the http box, enter the IPv4 or IPv6 address that was configured on the Transformer's Host or Network interface as the address to which the web browser must connect.

Note

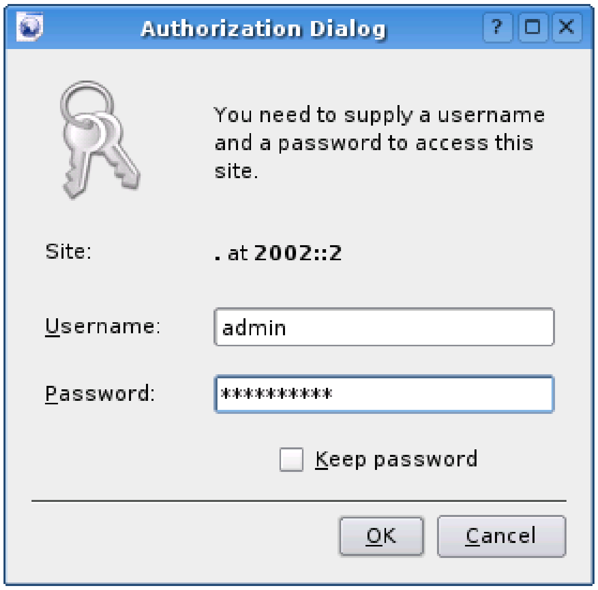
IPv6 addresses must be enclosed in brackets, e.g. http://[2002::2].



skf.datatekcorp.com - webGUI - Microsoft Internet Explorer provided by Datatek Applications Inc.

Address http://172.31.12.35/

3. The default user name is "**admin**" and the default password is "**mono**". The default login and password should be changed after logging in the first time. See General Setup page to configure new login and password.



Authorization Dialog

You need to supply a username and a password to access this site.

Site: . at 2002::2

Username: admin

Password: **********

□ Keep password

Passwords must conform to the following rules:

a. Passwords must have at least 10 case-sensitive characters.

b. Passwords must have a mix of uppercase letters, lowercase letters, numbers and special characters such that at least two characters from each of the afore-mentioned four types of characters are present.

For example: x$T1lTBn2! is a valid password.

Mv4*mabc3Z is *invalid* because it only has one special character.

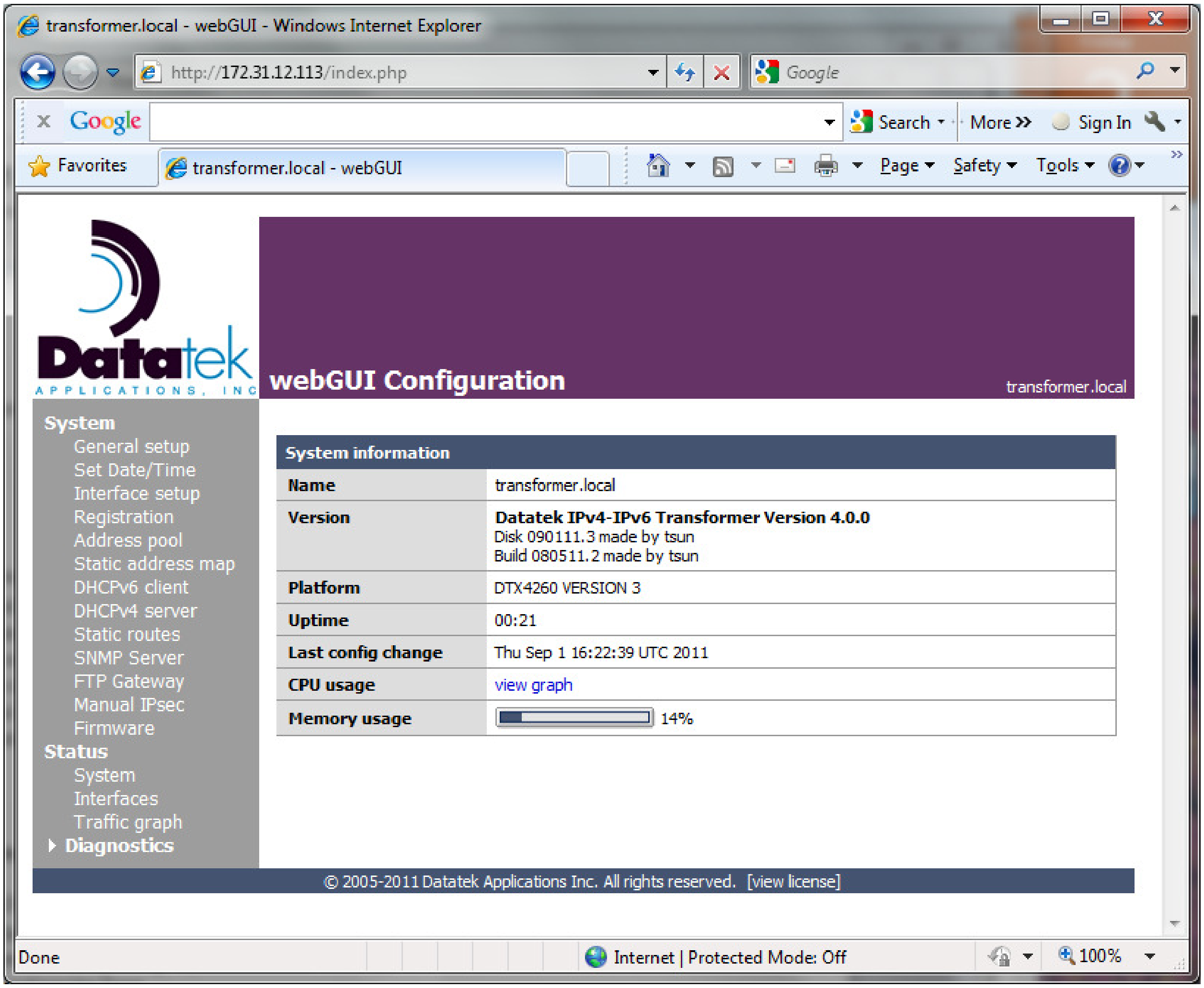
Mv4**abc3Z is *valid*.

c. New passwords must not be reused from any of the previous ten passwords.

Warning

Automatic expiration of passwords is not supported at this time.

4. After logging in, the Transformer's **Figure 7. System Information Screen** below will appear.



System information	
Name	transformer.local
Version	**Datatek IPv4-IPv6 Transformer Version 4.0.0** Disk 090111.3 made by tsun Build 080511.2 made by tsun
Platform	DTX4260 VERSION 3
Uptime	00:21
Last config change	Thu Sep 1 16:22:39 UTC 2011
CPU usage	view graph
Memory usage	14%

© 2005-2011 Datatek Applications Inc. All rights reserved. [view license]

Figure 7. System Information Screen

6 Logical Setup

6.1 Set up IPv4 and IPv6 interfaces

This selection lets you set the IP addresses and subnet masks/prefix lengths for the host and network side interfaces. This will allow you access to the webGUI. You must supply an IPv4 address and subnet mask for the host-side interface. You may also supply an IPv4 address/subnet mask and an IPv6 address/prefix length for the network-side interface. Note that these network-side addresses are for the management interface on the Transformer, not the proxy addresses for the legacy IPv4 device. You will need to use the webGUI to enter the proxy addresses.
We recommend using an IP address from the RFC1918 private address space for the host-side interface, since it's not visible to the network side of the Transformer. There are three private ranges:

Start	End
10.0.0.0	10.255.255.255
172.16.0.0	172.31.255.255
192.168.0.0	192.168.255.255

To configure the Transformer's interface, go to the Console main menu and select item 1- Set up IPv4 and IPv6 interfaces. In the example below, we set the host-side interface address to 192.168.1.1 and accept the default subnet mask length of 24. Note that each prompt shows the current or default value in parentheses. To accept the default value, simply press ENTER. Similarly, we set the network-side IPv6 and IPv4 addresses to 2007::50 and 135.47.8.16 respectively.

```
IPv4 address for host-side interface (172.31.0.1): 192.168.1.1
IPv4 subnet mask length for host-side interface (24):
IPv6 address for network-side interface, or "none" (none): 2007::50
IPv6 prefix length for 2007::50 (64):
IPv4 address for network-side interface, or "none" (none): 135.47.8.16
IPv4 subnet mask length for IPv6 LAN interface (16): 24

Please wait...
You can now access the webGUI by opening any of the following URLs
in your browser:

http://192.168.1.1/
http://[2007::50]/
http://135.47.8.16/

*** NOTE ***
You must reboot before these changes take effect.

Press ENTER to continue.
```

You aren't required to supply an IPv4 or IPv6 address for the network side interface. If you don't supply an IPv4 address, you won't be able to access the webGUI from the network-side interface using IPv4. If you don't supply an IPv6 address, you may still be able to access the webGUI using IPv6. This is because the network-side interface is automatically assigned an IPv6 link-local address.

Once you make changes to the host or network-side IP addresses, you must reboot the Transformer before the changes will take effect. To do this, from the Console Main Menu, select item 4, Reboot system.

6.2 Reset webGUI password

This selection resets the webGUI password to the factory default. To do this, from the Console Main Menu, select item 2 – Reset webGUI.

6.3 Reset to factory defaults

This selection resets all configured values to the factory defaults, including those that you have setup using the webGUI. Use it when you want to make a fresh start, like when you're moving a Transformer from one legacy device to another. To do this, from the Console Main Menu, select item 3 – Reset to factory defaults

Warning

Setting the unit back to the factory defaults will remove the registration key and a new one will need to be obtained from Datatek

6.4 Reboot system

This selection reboots the Transformer. To do this, from the Console Main Menu, select item 4 – Reboot system.

6.5 Ping host

This selection allows you to enter either a hostname or IP address of a target machine that you wish to ping. To do this, from the Console Main Menu, select item 5 – Ping host. The IP address can be either an IPv4 or IPv6 address. However, Ping6 directed to the legacy host will not work.

6.6 Change password

This selection allows you to change the password to the serial console. To do this, from the Console Main Menu, select item 6 – Change password. You may not use the null password anymore. Any password selection is acceptable. There are no rules on the length of the password nor use of special characters.

6.7 Logoff

This selection allows you to logoff from the serial console. To do this, from the Console Main Menu, select item 7 – Logoff. After you logoff, you will be prompted to Login.

7 Software Registration

The Transformer must be registered before IPv4-IPv6 transforming will work. Without registration, configuration can still be set up, except for pool and bindings. IPv6 and IPv4 access to the web server will still work.

The Transformer will ship from Datatek with a valid registration key. When upgrading the Transformer to a major new release, a new registration key will need to be obtained from Datatek. Minor release updates will not require a new key.

To perform Registration, go to the WebGUI System page. Click on the Registration button from the menu on the left side of the page, and the Registration form will be displayed, as shown in **Figure 8. Registration Screen.**

The registration page has three main fields:

1. Product ID
2. Software version
3. Authorization code to be entered by the user.

The product ID and software version should be provided to Datatek, and the authorization code obtained from Datatek should be entered into the Authorization code field.

The user must reboot upon successfully entering the Authorization code. The "reboot" indicator is displayed on most web pages, and the "not registered" indicator is removed.

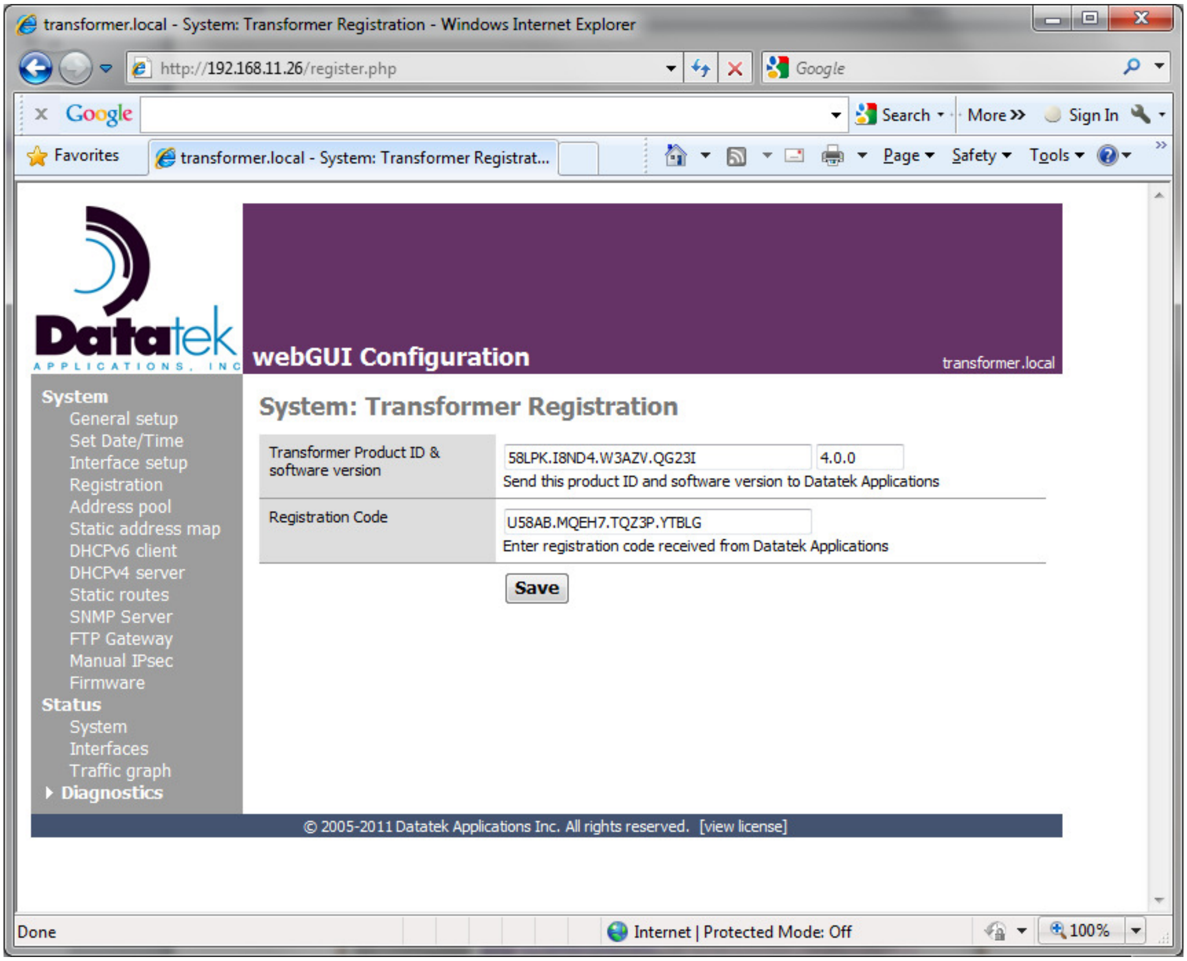
Warning

Setting the unit back to the factory defaults will remove the authorization code and a new one will need to be obtained from Datatek

To obtain an Authorization Code you may contact Datatek at:

Datatek Applications, Inc
399 Campus Drive
Suite 140
Somerset, NJ 08873
Phone 732-667-1080
www.datatekcorp.com
ipv6support@datatekcorp.com

Figure 8. Registration Screen displays the Transformer Product ID and Software Version and a field where the user must enter the Registration Code



System: Transformer Registration

Transformer Product ID & software version	58LPK.I8ND4.W3AZV.QG23I 4.0.0 Send this product ID and software version to Datatek Applications
Registration Code	U58AB.MQEH7.TQZ3P.YTBLG Enter registration code received from Datatek Applications

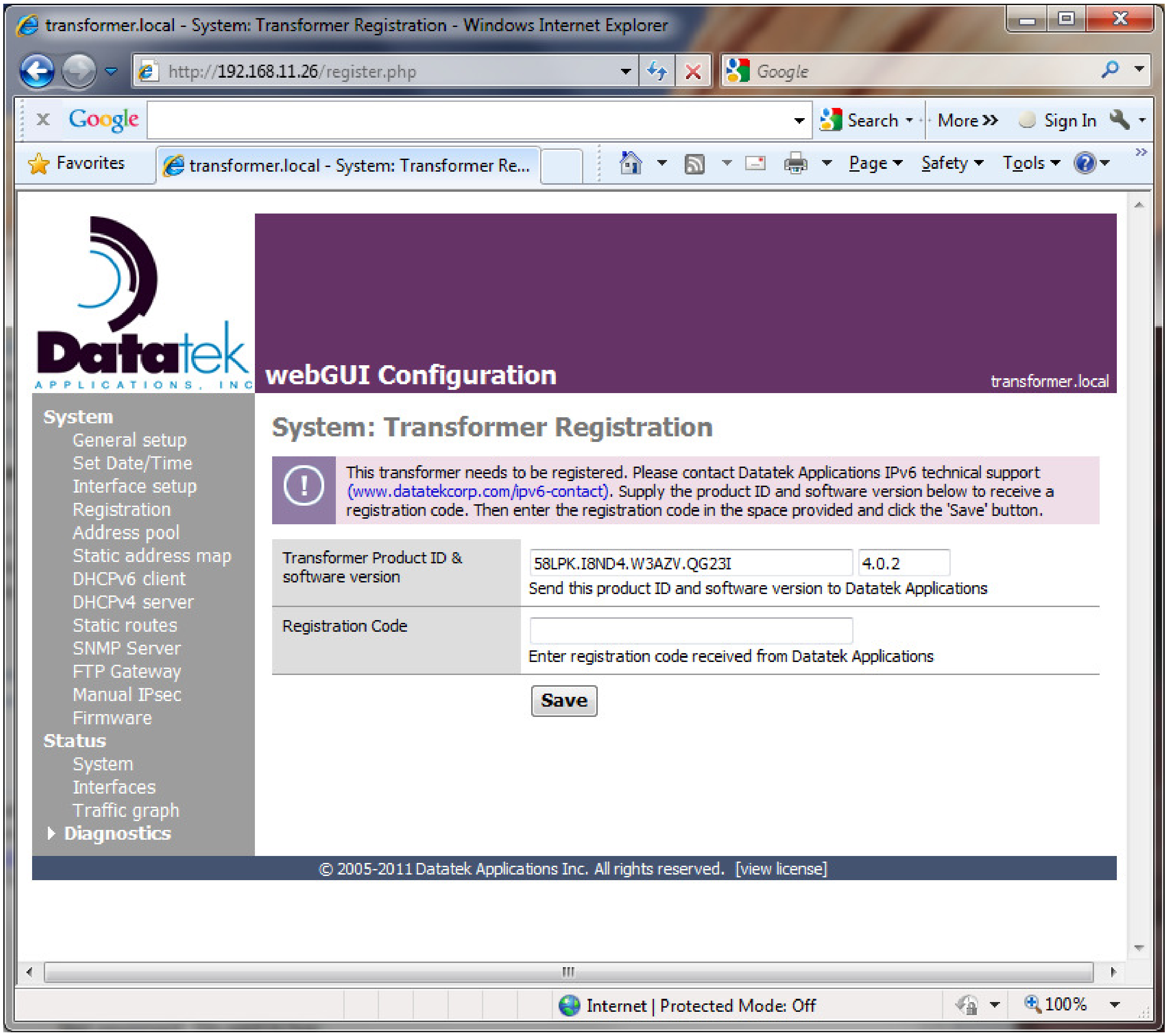
© 2005-2011 Datatek Applications Inc. All rights reserved. [view license]

Figure 8. Registration Screen

If registration has not been done or the user has entered an invalid Registration Code, most of the web pages will show an added information block near the top. The info block contains a link to the registration page.

The registration page is where the user carries out the registration process. The "not registered" information block and the side frame of every page of the web interface both have links to the registration page.

Figure 9. Unregistered Transformer Screen appears if the user has entered an invalid Registration Code.



System: Transformer Registration

This transformer needs to be registered. Please contact Datatek Applications IPv6 technical support (www.datatekcorp.com/ipv6-contact). Supply the product ID and software version below to receive a registration code. Then enter the registration code in the space provided and click the 'Save' button.

Transformer Product ID & software version	58LPK.I8ND4.W3AZV.QG23I 4.0.2 Send this product ID and software version to Datatek Applications
Registration Code	Enter registration code received from Datatek Applications

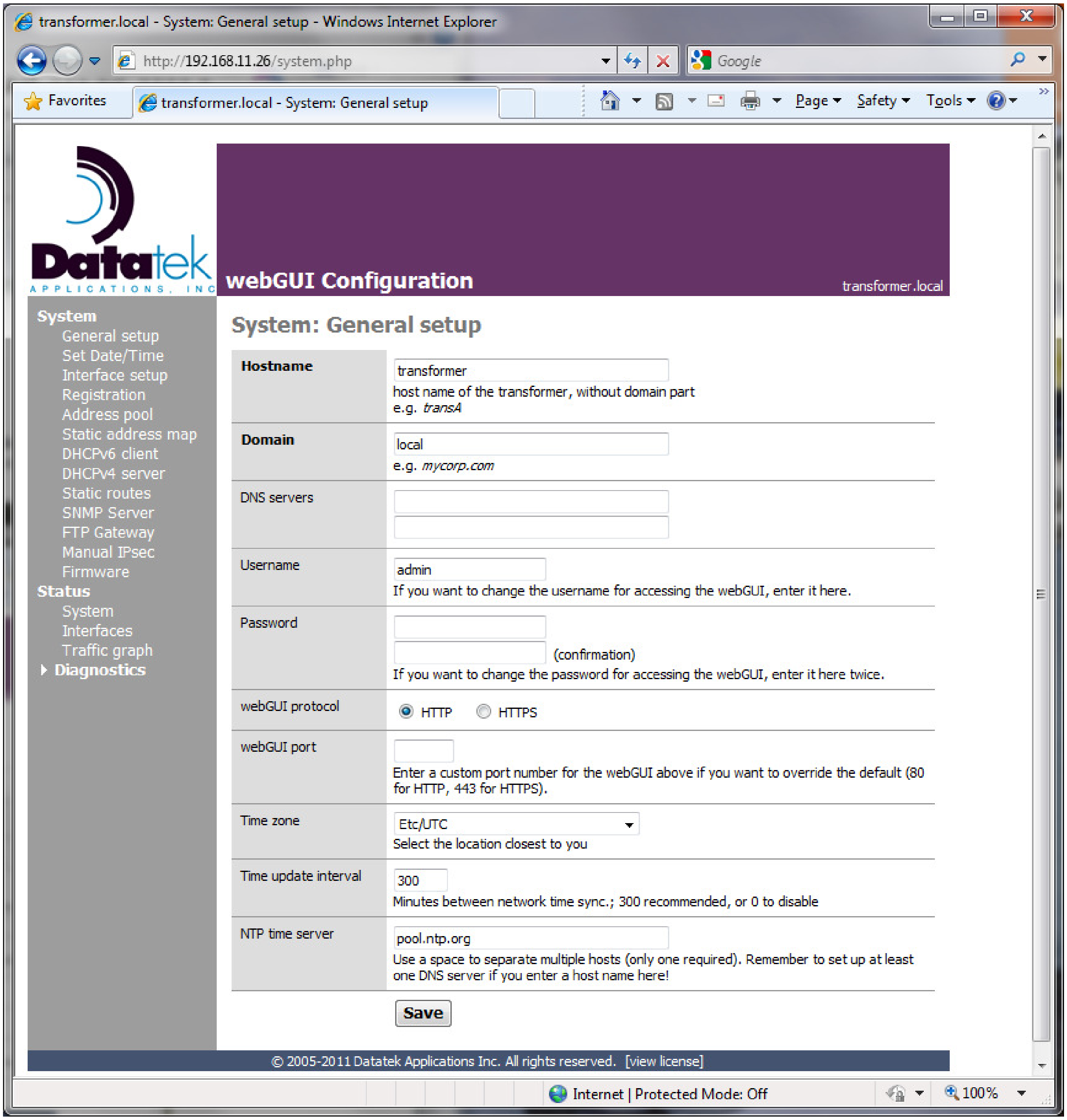
© 2005-2011 Datatek Applications Inc. All rights reserved. [view license]

Figure 9. Unregistered Transformer Screen

8 Web Graphical User Interface (webGUI) System

8.1 General Setup

The **Figure 10. General setup Screen** below displays configurable information that applies to the entire Transformer as a whole, rather than to a specific interface, address or feature.



System: General setup

Hostname	transformer host name of the transformer, without domain part e.g. *transA*
Domain	local e.g. *mycorp.com*
DNS servers	
Username	admin If you want to change the username for accessing the webGUI, enter it here.
Password	(confirmation) If you want to change the password for accessing the webGUI, enter it here twice.
webGUI protocol	● HTTP ○ HTTPS
webGUI port	Enter a custom port number for the webGUI above if you want to override the default (80 for HTTP, 443 for HTTPS).
Time zone	Etc/UTC Select the location closest to you
Time update interval	300 Minutes between network time sync.; 300 recommended, or 0 to disable
NTP time server	pool.ntp.org Use a space to separate multiple hosts (only one required). Remember to set up at least one DNS server if you enter a host name here!

© 2005-2011 Datatek Applications Inc. All rights reserved. [view license]

Figure 10. General setup Screen

Hostname

This is the name of the Transformer.

Domain

This is the domain of the Transformer.

DNS servers

This is the IP address of the DNS Server, both a primary and secondary are allowed. When the Transformer receives a DNS lookup request for a hostname from the IPv4 legacy device the request is turned into a request for an IPv6 address and is sent to the DNS Server. The IPv6 address received from the DNS Server is then mapped to a dynamic IPv4 address. The dynamically bound IPv4 address is returned to the IPv4 legacy device as the response to its original lookup request.

Username

This is the login name of the administrator. It is the same as the Username in the popup authorization dialog that appears when one first connects to the webGUI.

Password

To change the current password, type in a new password. It is the same one that is used in the authorization dialog that appears when one first connects to the webGUI.

Passwords must conform to the following rules:

Passwords must have at least 10 case-sensitive characters.
Passwords must have a mix of uppercase letters, lowercase letters, numbers and special characters.
Passwords must have at least two characters from each of the afore-mentioned four types of characters.

For example:

x$T1lTBn2! is a *valid* password.
Mv4*mabc3Z is *invalid* because it only has one special character.
Mv4**abc3Z is *valid*.

New passwords must not be reused from any of the previous ten passwords.

Warning

Automatic expiration of passwords is not supported at this time.

SAVE

A domain must be entered before the information on this screen can be saved. Select the **SAVE** button before proceeding to the remaining configuration screens, otherwise the information will be lost. Furthermore, configuration on the **General setup** screen determines the availability of some options on the other screens.

Note

A reboot is required for any configuration changes made on the other screens to take effect. The GUI will display instances when a reboot is required.

webGUI protocol

Select HTTP or HTTPS as the GUI protocol. HTTPS uses HTTP over SSL (Secure Socket Layer) for security.

webGUI port

Enter a custom HTTP port number to use or leave blank to use the default port of 80 for HTTP and 443 for HTTPS.

Time zone

Select the time zone the Transformer is in.

Time update interval

Enter how often the Transformer should use NTP (Network Time Protocol) to synchronize its clock with a server in the network.

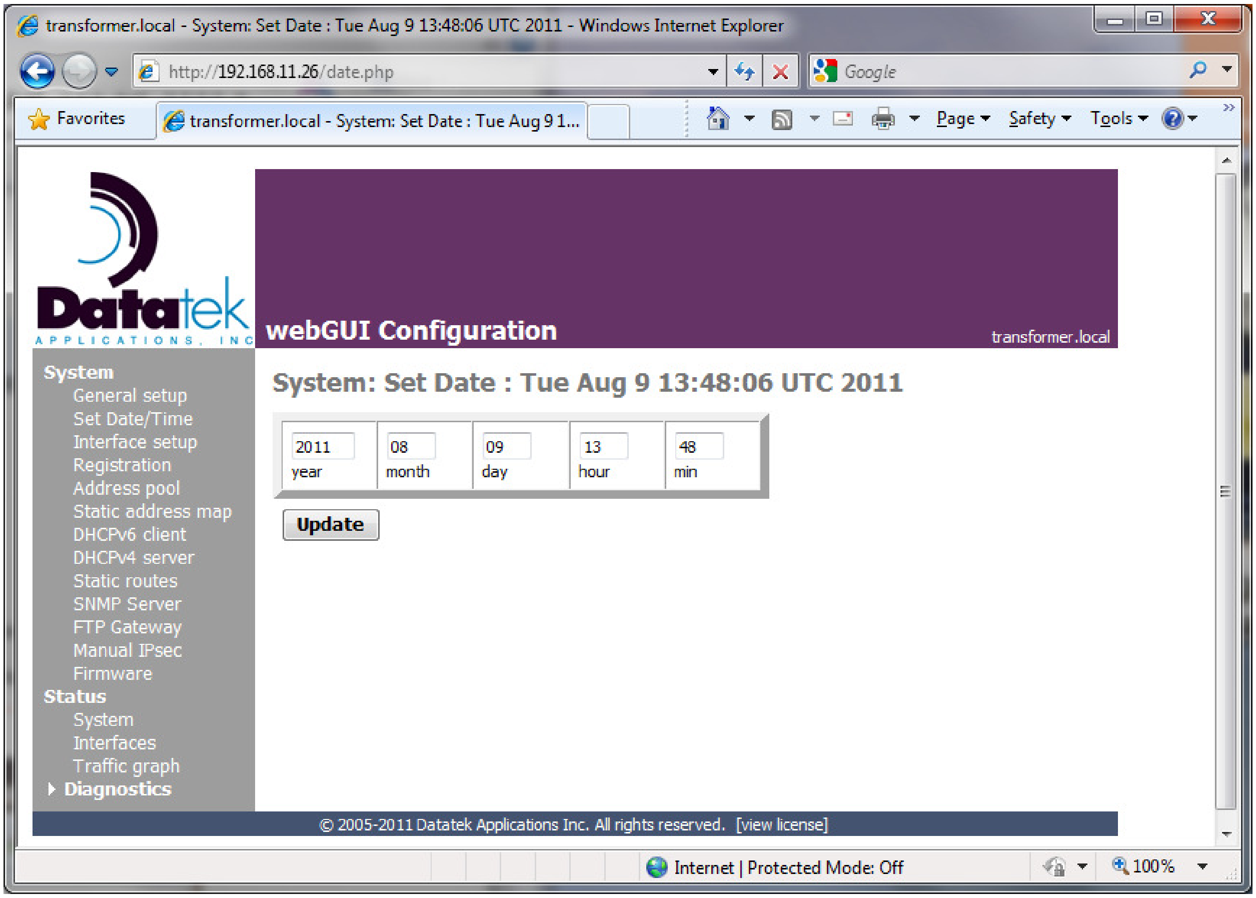
NTP time server

Enter the domain name of the NTP (Network Time Protocol) time server.

Set Date/Time

The **Set Date/Time** form allows the user to configure the date and time on the Transformer.

Enter the current year, month, day, hour and minute in the format displayed in **Figure 11. Set Date/Time Screen** and select Update to apply the changes.



transformer.local - System: Set Date : Tue Aug 9 13:48:06 UTC 2011 - Windows Internet Explorer

http://192.168.11.26/date.php

System: Set Date : Tue Aug 9 13:48:06 UTC 2011

2011	08	09	13	48
year	month	day	hour	min

© 2005-2011 Datatek Applications Inc. All rights reserved. [view license]

Figure 11. Set Date/Time Screen

8.2 Interface Setup

The **Interface setup form** is used to configure the host-side and network-side interfaces of the Transformer and the IPv4 address of the legacy device and the proxy IPv6 address of the legacy device.

There are two interfaces on the Transformer, a host-side interface and a network-side interface. If the legacy device is manually configured, its configuration should be set up to match the configuration entered in this form. If the legacy device is configured to receive its configuration automatically, the values it receives come from the entries in this form.

Figure 13. Interface setup screen shows all the configuration fields and options.

8.3 Host-side

Device IPv4 address

This is the IPv4 address of the legacy device.

Transformer IPv4 address

This is the IPv4 address of the Transformer's host-side interface.

8.4 Network-side

Device IPv6 address

This is the IPv6 proxy address of the legacy device. This IPv6 proxy address is bound to the IPv4 address of the legacy device. In translating IPv4 packets from the legacy device, the IPv4 device address is translated to the IPv6 proxy address.

Transformer IPv6 address

This is the IPv6 address of the Transformer. This is one of the addresses to which the web browser may connect in order to talk to the Transformer's web server. The other address the web browser may use is the **Transformer IPv4 address.**

Device IPv4 address

This is an IPv4 address for the legacy device that appears on the network-side interface. Nodes on the network side that wish to talk to the legacy device must use this address. This IPv6 proxy address is bound to the IPv4 address of the legacy device. In translating IPv4 packets from the legacy device, the IPv4 device address is translated to the IPv6 proxy address.

Transformer IPv4 address

This is the IPv4 address of the Transformer on the network-side interface. This is one of the addresses to which the web browser may connect in order to talk to the Transformer's web server. The other address the web browser may use is the IPv4 address on the host side.

Figure 12. Example Network Setup displays all the interfaces and their IPv4 and IPv6 addresses that are of interest to the Transformer. The diagram uses the sample addresses that were configured in the Interface screen capture **Figure 13. Interface setup Screen.**

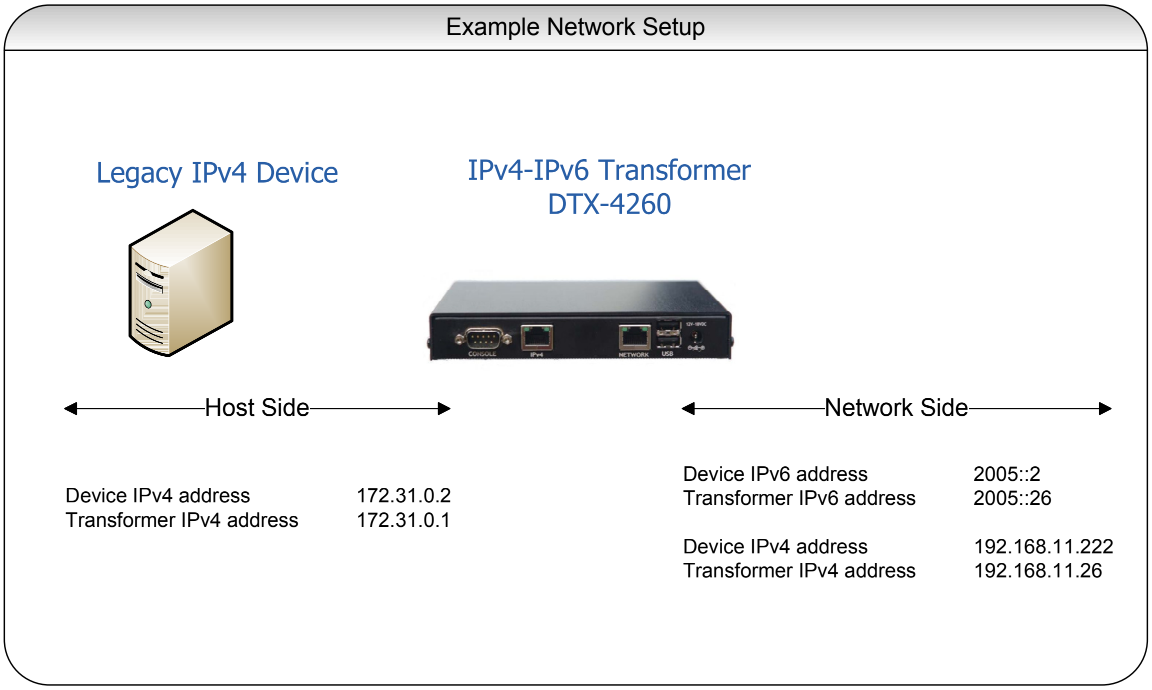

Example Network Setup
Legacy IPv4 Device
IPv4-IPv6 Transformer
DTX-4260
CONSOLE
IPv4
NETWORK
USB
Host Side
Network Side
Device IPv4 address 172.31.0.2
Transformer IPv4 address 172.31.0.1
Device IPv6 address 2005::2
Transformer IPv6 address 2005::26
Device IPv4 address 192.168.11.222
Transformer IPv4 address 192.168.11.26

Figure 12. Example Network Setup

Accept router advertisements

This is checked to enable stateless address autoconfiguration as specified in RFC4862. If this is not checked, the Transformer must get its IPv6 address through alternative means such as manual configuration through the Transformer IPv6 Address field or through stateful address configuration like DHCPv6.

Use temporary addresses

This is checked to make the IEEE interface identifiers and the random number which are both used in generating the global IPv6 addresses from stateless address autoconfiguration to change over time as specified in RFC3041. The interface identifiers are made to change over time by generating random values that will cause the IPv6 global address to also change over time, making it more difficult for eavesdroppers and affording more privacy.

Prefer temporary addresses

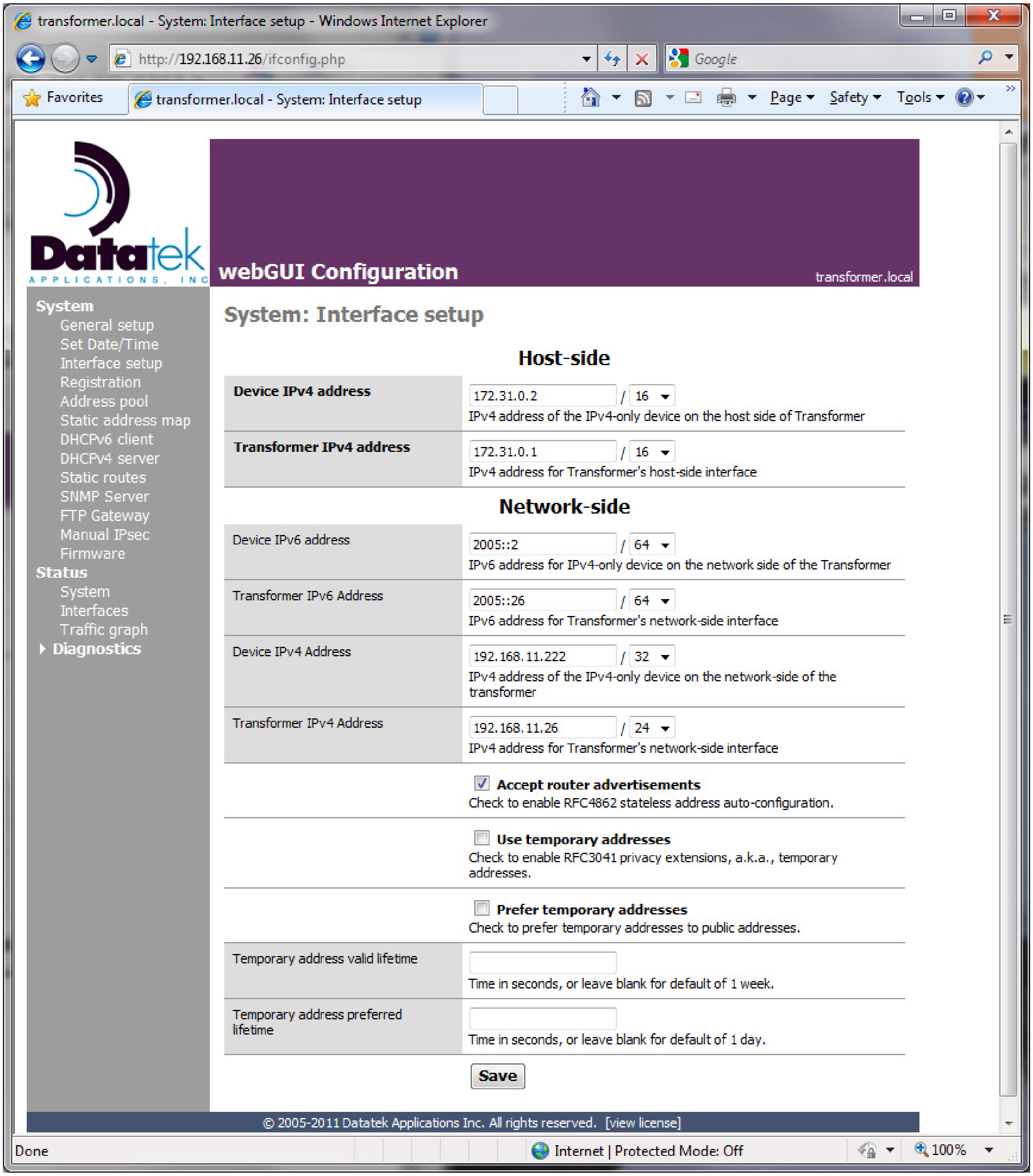
This is checked to give preference to temporary addresses over public addresses in source address selection when connections are initiated from the Transformer itself or from the host-side legacy device.

Temporary address valid lifetime

Enter the valid lifetime of the temporary address in seconds or leave blank for the default of 1 week.

Temporary address preferred lifetime

Enter the preferred lifetime of the temporary address in seconds or leave blank for the default of 1 day.



System: Interface setup

Host-side

Device IPv4 address	172.31.0.2 / 16 IPv4 address of the IPv4-only device on the host side of Transformer
Transformer IPv4 address	172.31.0.1 / 16 IPv4 address for Transformer's host-side interface

Network-side

Device IPv6 address	2005::2 / 64 IPv6 address for IPv4-only device on the network side of the Transformer
Transformer IPv6 Address	2005::26 / 64 IPv6 address for Transformer's network-side interface
Device IPv4 Address	192.168.11.222 / 32 IPv4 address of the IPv4-only device on the network-side of the transformer
Transformer IPv4 Address	192.168.11.26 / 24 IPv4 address for Transformer's network-side interface
	☑ **Accept router advertisements** Check to enable RFC4862 stateless address auto-configuration.
	☐ **Use temporary addresses** Check to enable RFC3041 privacy extensions, a.k.a., temporary addresses.
	☐ **Prefer temporary addresses** Check to prefer temporary addresses to public addresses.
Temporary address valid lifetime	Time in seconds, or leave blank for default of 1 week.
Temporary address preferred lifetime	Time in seconds, or leave blank for default of 1 day.

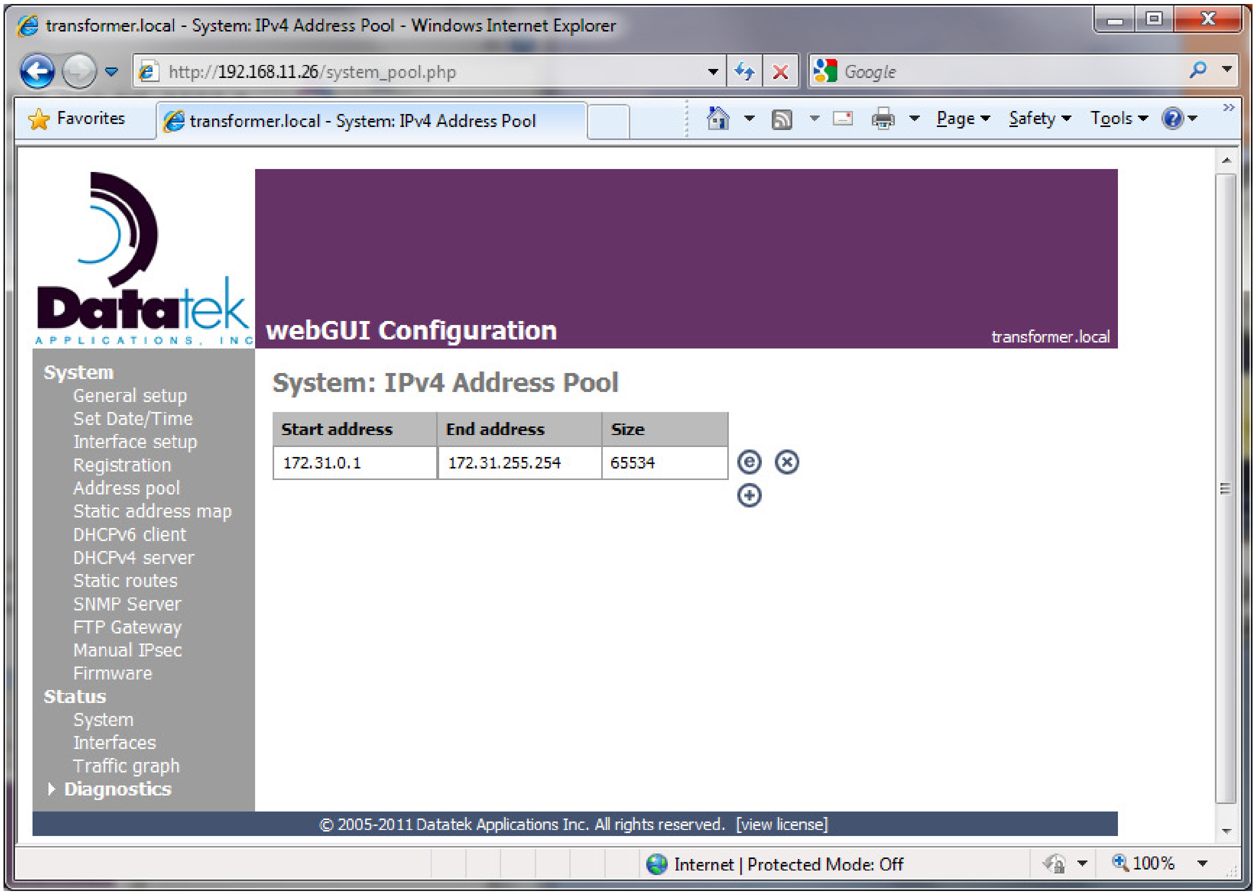
Figure 13. Interface setup screen

8.5 Address pool

The **Address pool** form displays the starting and ending addresses of ranges of IPv4 addresses that are used to automatically map an IPv6 address in an IPv6 packet received from the network side to an IPv4 address so that the IPv6 packet can be translated to IPv4 and forwarded to the IPv4 legacy host.

The address pool may be configured in any way that does not conflict with the IPv4 addressing on the network side. The best approach is to choose an address pool that is in the same subnetwork as the one containing the host IP and the host-side Transformer IP addresses. This should be in one of the private subnetwork ranges and should not appear in the address space reachable on the network side.

The IPv4 Address Pool Screen is displayed in **Figure 14. IPv4 Address Pool Screen**



System: IPv4 Address Pool

Start address	End address	Size
172.31.0.1	172.31.255.254	65534

Figure 14. IPv4 Address Pool Screen

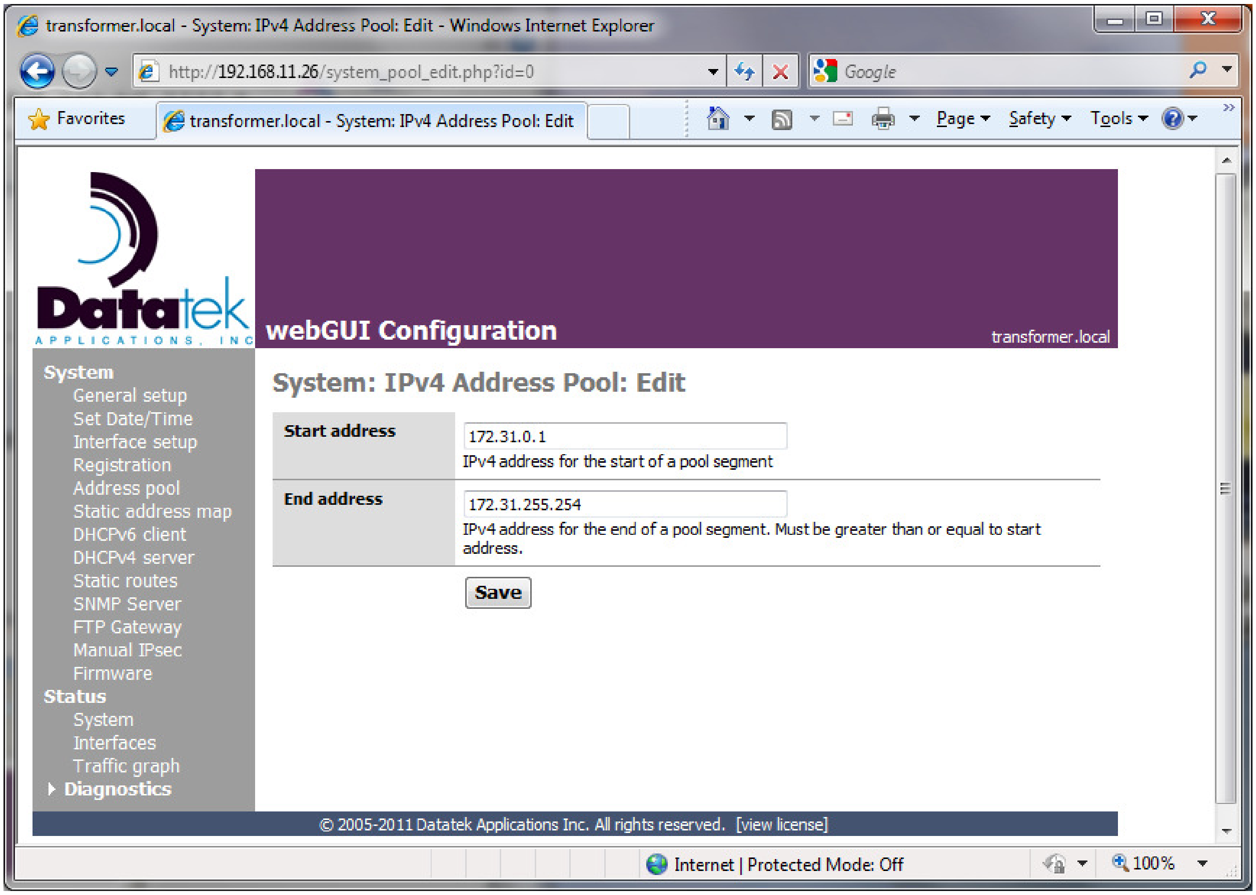
The following buttons are provided for editing the entries in the address pool:

⊕ Add a new range of IPv4 addresses to the pool.

ⓔ Edit an existing range.

⊗ Delete an existing range.

Figure 15. Adding or Editing the Address Pool Screen is displayed when a new address range is added or an existing address range is edited.



transformer.local - System: IPv4 Address Pool: Edit - Windows Internet Explorer

http://192.168.11.26/system_pool_edit.php?id=0

System: IPv4 Address Pool: Edit

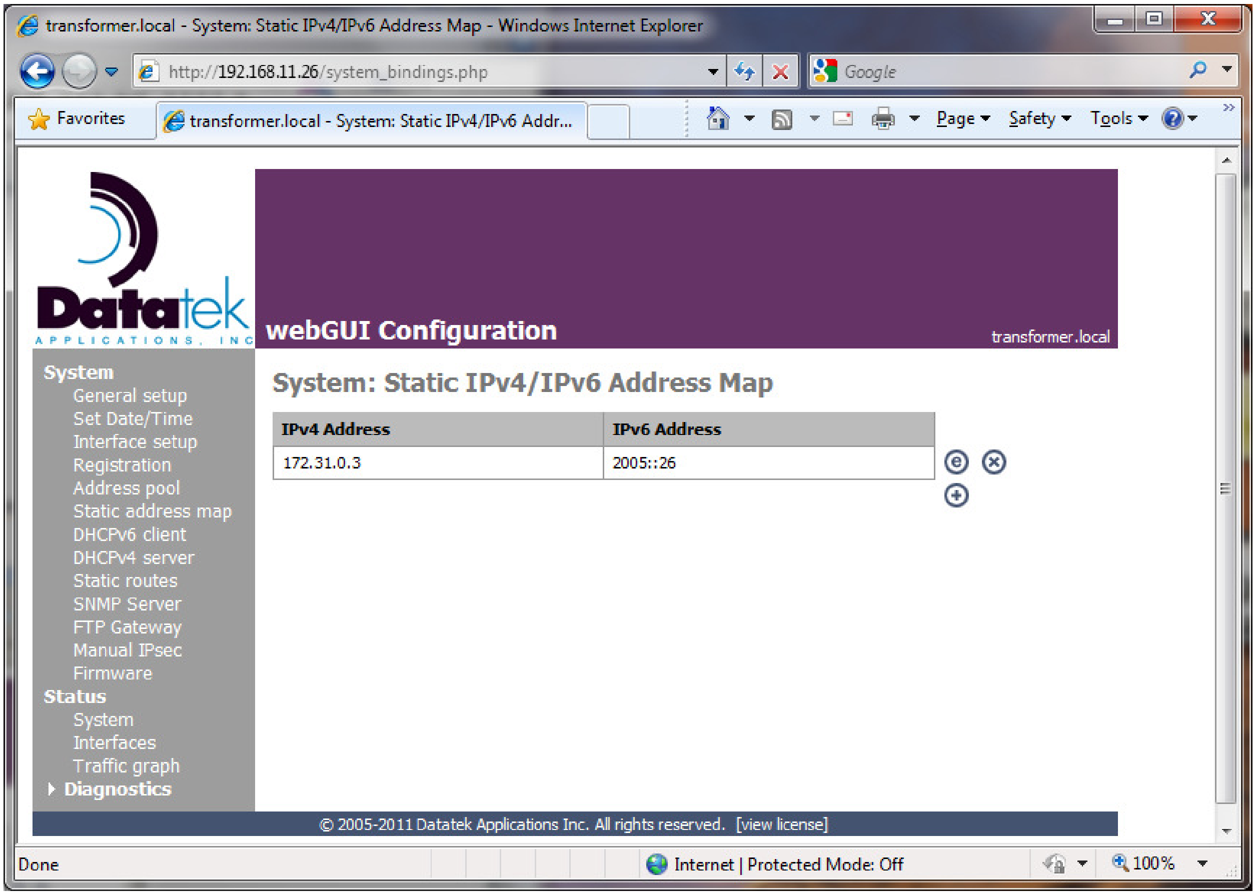
Start address	172.31.0.1 IPv4 address for the start of a pool segment
End address	172.31.255.254 IPv4 address for the end of a pool segment. Must be greater than or equal to start address.

© 2005-2011 Datatek Applications Inc. All rights reserved. [view license]

Figure 15. Adding or Editing the Address Pool Screen

8.6 Static address map

Figure 16. Static IPv4/IPv6 Address Map Screen displays manually configured bindings between the IPv4 and IPv6 addresses. The legacy IPv4 host reaches these given IPv6 addresses using the given IPv4 addresses. These static bindings may use IPv4 addresses that are in the pool or not in the pool, but they should not be reachable on the network side.



transformer.local - System: Static IPv4/IPv6 Address Map - Windows Internet Explorer
http://192.168.11.26/system_bindings.php
Google
Favorites
transformer.local - System: Static IPv4/IPv6 Addr...
Page
Safety
Tools
Datatek APPLICATIONS, INC
webGUI Configuration
transformer.local
System
General setup
Set Date/Time
Interface setup
Registration
Address pool
Static address map
DHCPv6 client
DHCPv4 server
Static routes
SNMP Server
FTP Gateway
Manual IPsec
Firmware
Status
System
Interfaces
Traffic graph
Diagnostics
© 2005-2011 Datatek Applications Inc. All rights reserved. [view license]
Done
Internet | Protected Mode: Off
100%

System: Static IPv4/IPv6 Address Map

IPv4 Address	IPv6 Address
172.31.0.3	2005::26

Figure 16. Static IPv4/IPv6 Address Map Screen

⊕ Add a static binding between an IPv4 and IPv6 address to the table.

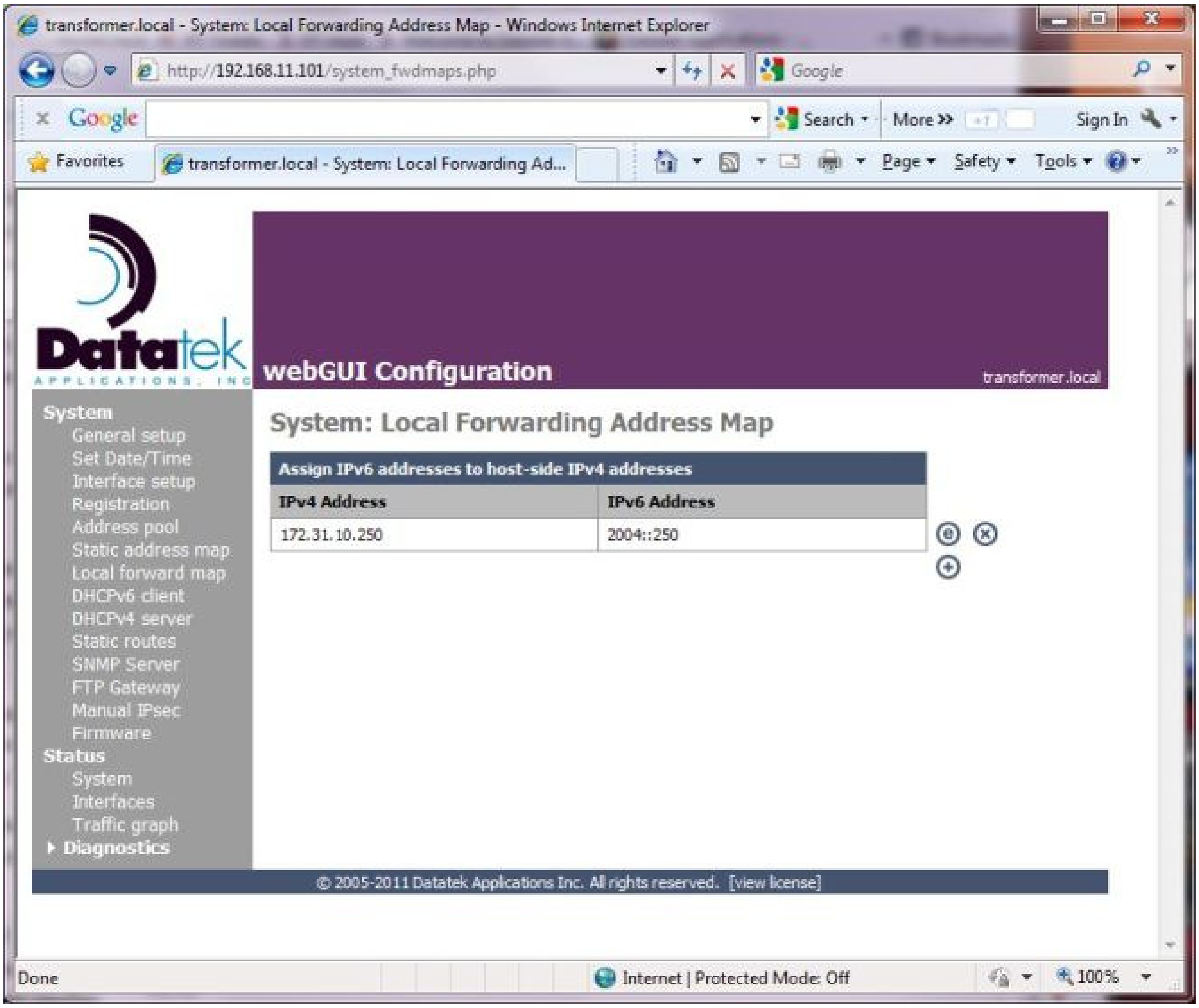
ⓔ Edit an existing static binding.

⊗ Delete an existing static binding.

8.7 Local Forwarding address map

This feature configures bindings that allow additional IPv4 hosts to communicate with IPv6 endpoints. As shown in **Figure 17. Local Forwarding Address Map Screen,** enter the local (host-side) addresses of the IPv4 hosts and the IPv6 addresses by which they will be known to the network side. Note, no autoconfiguration will be done by the Transformers for these additional hosts.

`



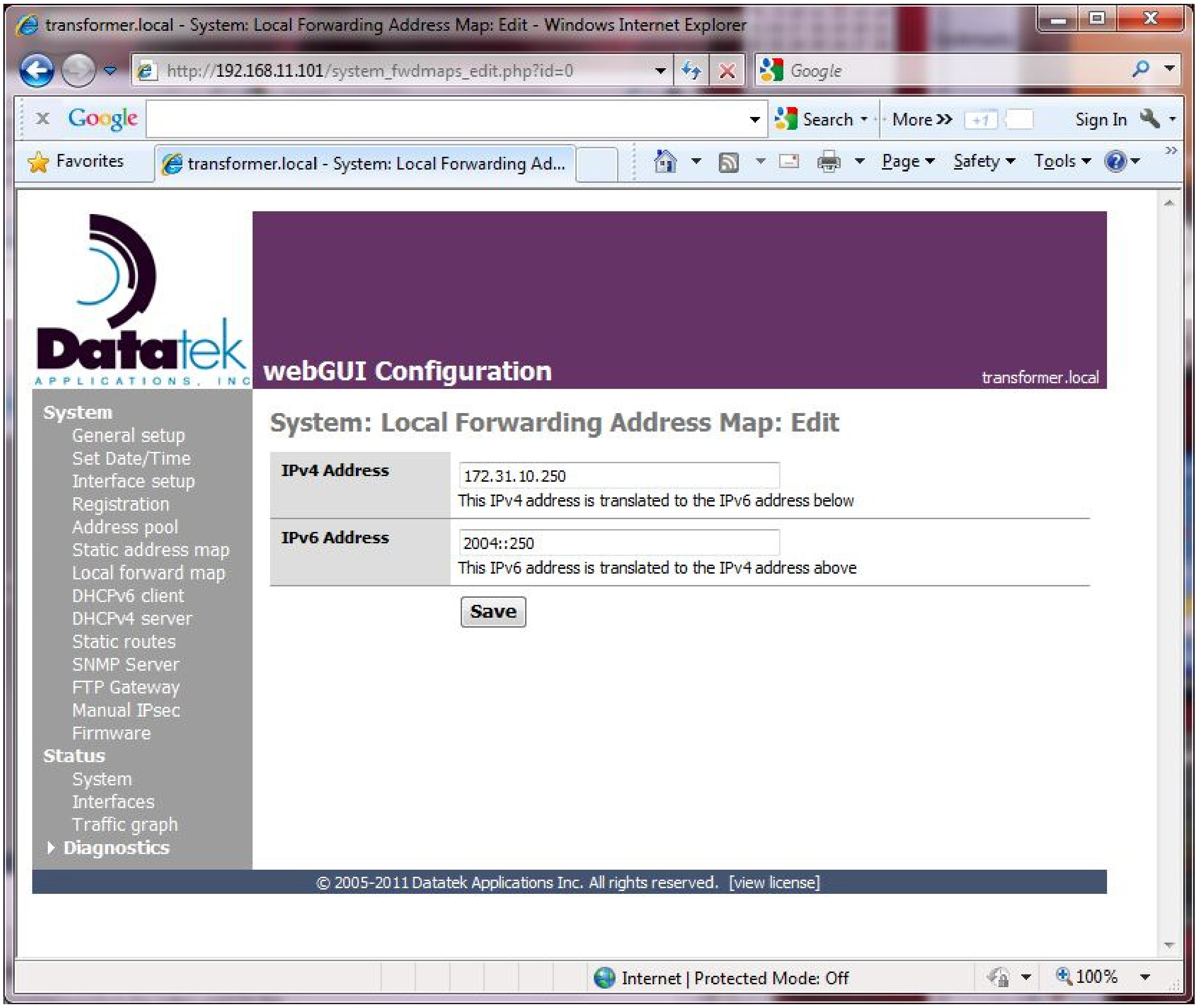
System: Local Forwarding Address Map

Assign IPv6 addresses to host-side IPv4 addresses

IPv4 Address	IPv6 Address
172.31.10.250	2004::250

Figure 17. Local Forwarding Address Map Screen

Figure 18. Local Forwarding Address Map Edit Screen is displayed when a new address range is added or an existing address range is edited.



System: Local Forwarding Address Map: Edit

IPv4 Address	172.31.10.250 This IPv4 address is translated to the IPv6 address below
IPv6 Address	2004::250 This IPv6 address is translated to the IPv4 address above

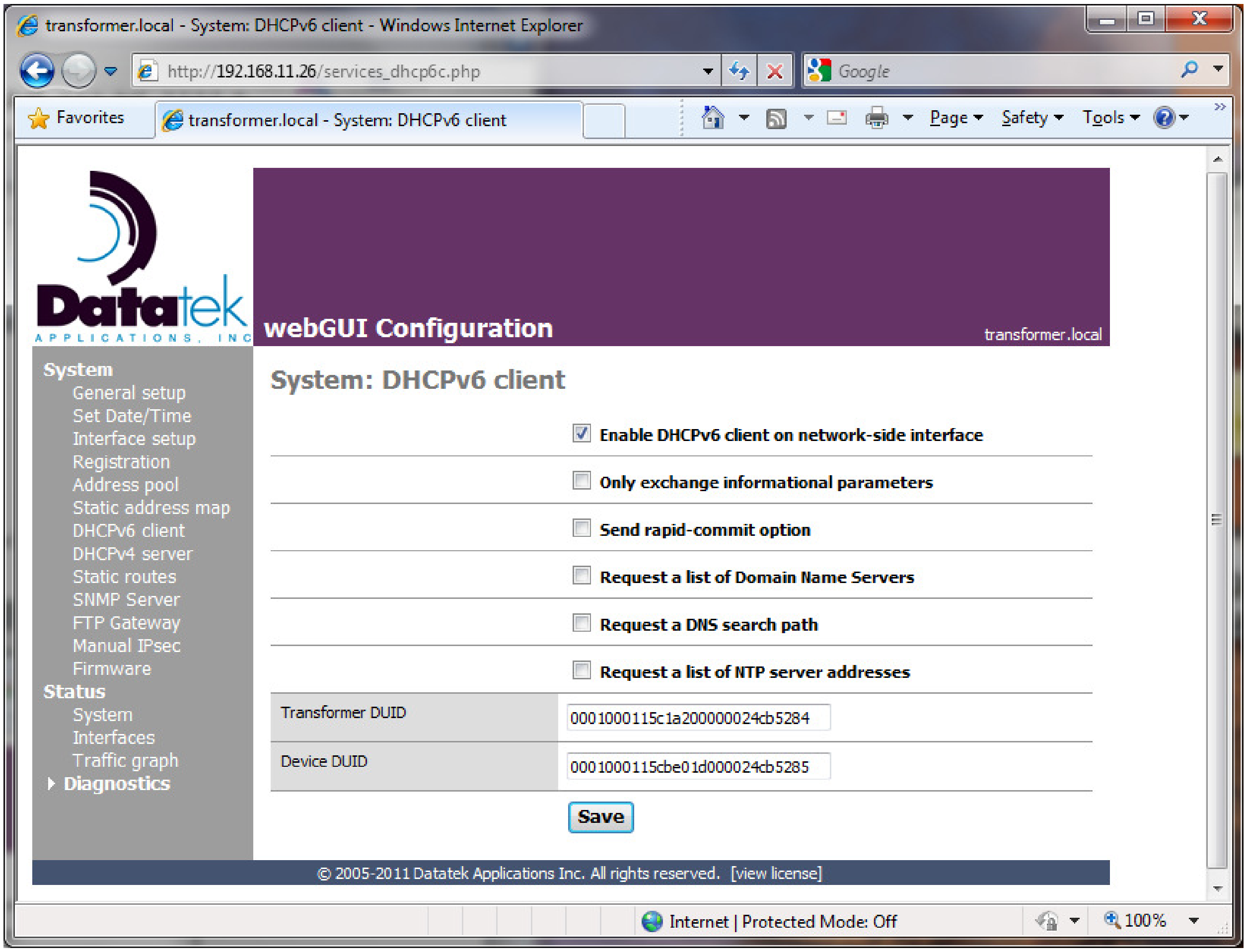
Save

© 2005-2011 Datatek Applications Inc. All rights reserved. [view license]

Figure 18. Local Forwarding Address Map Edit Screen

8.8 DHCPv6 client

The Transformer can be enabled to act as a DHCPv6 client to some DHCPv6 server on the IPv6 network side. The DHCPv6 client Screen is displayed in **Figure 19. DHCPv6 client Screen.**



System: DHCPv6 client

☑ Enable DHCPv6 client on network-side interface

☐ Only exchange informational parameters

☐ Send rapid-commit option

☐ Request a list of Domain Name Servers

☐ Request a DNS search path

☐ Request a list of NTP server addresses

Transformer DUID	0001000115c1a200000024cb5284
Device DUID	0001000115cbe01d000024cb5285

© 2005-2011 Datatek Applications Inc. All rights reserved. [view license]

Figure 19. DHCPv6 client Screen

Enable DHCPv6 client on network-side interface

This checkbox is selected to enable the Transformer to act as a DHCPv6 client.

Only exchange informational parameters

This checkbox is selected to receive only the informational parameters that appear below. That is, the DHCPv6 server is to serve IPv6 addresses as well as the informational parameters described below to the Transformer.

Send Rapid-Commit option

This checkbox is selected for the Transformer to send DHCPv6 messages with the Rapid Commit option.

Request a list of Domain Name Servers

This checkbox is selected for the Transformer to request a list of DNS addresses from the DHCPv6 server.

Request a DNS search path

This checkbox is selected to request a DNS search path by domain name from the DHCPv6 server.

Request a list of NTP server addresses

This checkbox is selected to request a list of NTP server addresses from the DHCPv6 server.

Transformer DUID

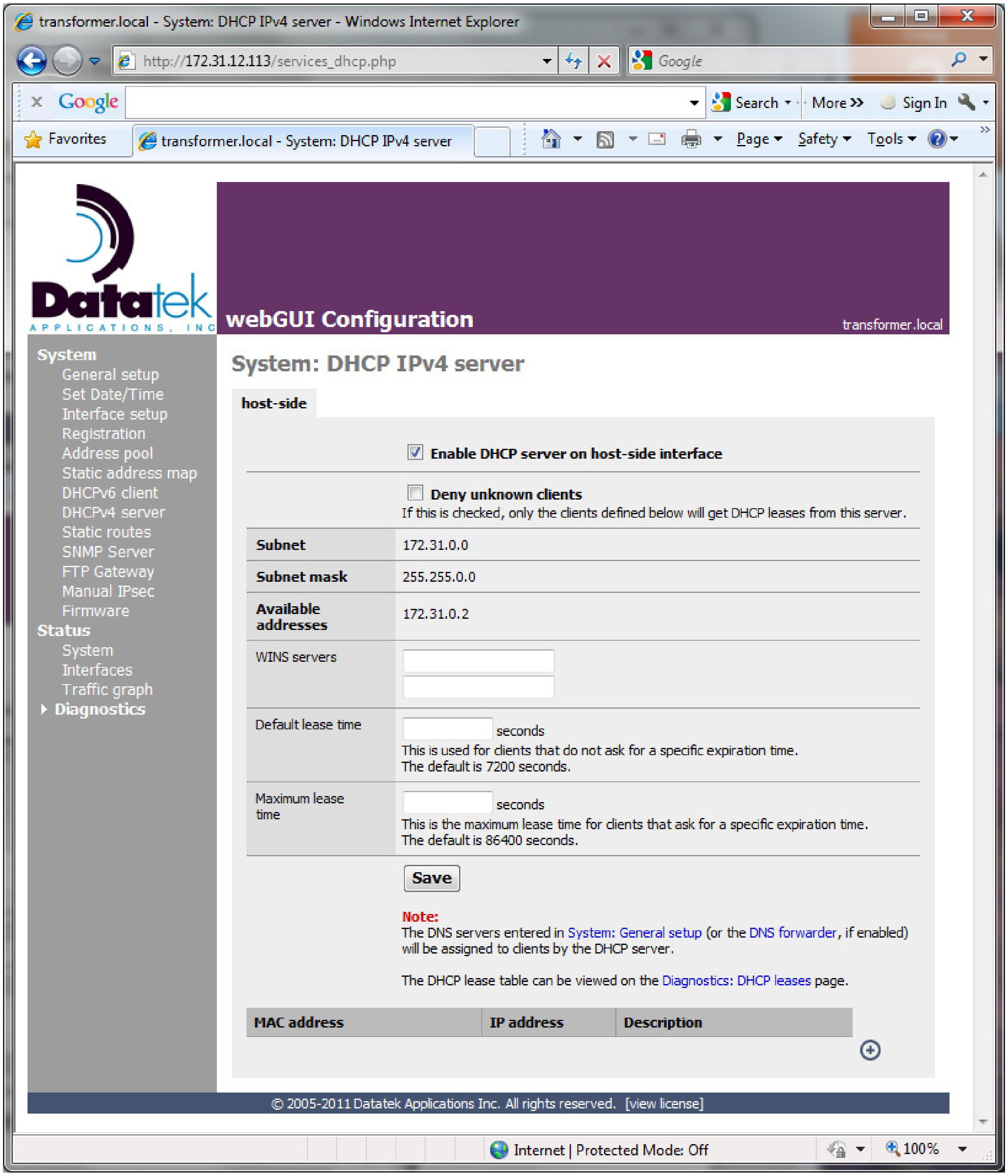
Change the DHCP Unique Identifier (DUID) of the Transformer to a DUID by which the DHCPv6 server knows the Transformer. A default DUID is automatically created at boot time and displayed in this field.

Device DUID

Change the DHCP Unique Identifier (DUID) of the legacy IPv4 device to a DUID by which the DHCPv6 server knows the legacy device. A default DUID is automatically created at boot time and displayed in this field.

8.9 DHCPv4 server

The Transformer can act as a DHCPv4 Server to the IPv4 legacy host to provide host configuration parameters to the IPv4 legacy host. The DHCPv4 server Screen is displayed in **Figure 20. DHCPv4 server Screen.**



System: DHCP IPv4 server

☑ Enable DHCP server on host-side interface

□ Deny unknown clients
If this is checked, only the clients defined below will get DHCP leases from this server.

Subnet	172.31.0.0
Subnet mask	255.255.0.0
Available addresses	172.31.0.2
WINS servers	
Default lease time	seconds This is used for clients that do not ask for a specific expiration time. The default is 7200 seconds.
Maximum lease time	seconds This is the maximum lease time for clients that ask for a specific expiration time. The default is 86400 seconds.

Note:
The DNS servers entered in System: General setup (or the DNS forwarder, if enabled) will be assigned to clients by the DHCP server.

The DHCP lease table can be viewed on the Diagnostics: DHCP leases page.

MAC address	IP address	Description

© 2005-2011 Datatek Applications Inc. All rights reserved. [view license]

Figure 20. DHCPv4 server Screen

Enable DHCP server on host-side interface

This checkbox is selected to enable the Transformer to act as a DHCPv4 server to the legacy IPv4 device and to locally forwarded IPv4 endpoints.

Deny unknown clients

Select this checkbox to allow DHCP to assign IP addresses only to the clients with MAC addresses entered in the table below. When locally forwarded endpoints are used with DHCP, this checkbox must be selected and the static address assignment list must be used to assign the IP and MAC addresses of the primary host and each of the secondary hosts.

Subnet

The subnet on which the legacy IPv4 host resides is displayed. This field is taken from the Interface Setup's screen's host-side configuration.

Subnet mask

This is the subnet mask of the above subnet. This field is taken from the Interface Setup's screen's host-side configuration.

Available addresses

This is the IPv4 address that the Transformer serves to the legacy host. This field is taken from the Interface Setup's screen's host-side configuration.

WINS server

These are the IPv4 addresses of the WINS server(s) that the Transformer serves to the legacy host.

Default lease time

This is the number of seconds for which the parameters served to the legacy host remain valid. The default is 7200 seconds.

Maximum lease time

This is the maximum number of seconds for which the parameters served to the legacy host remain valid. The default is 86,400 seconds.

Note

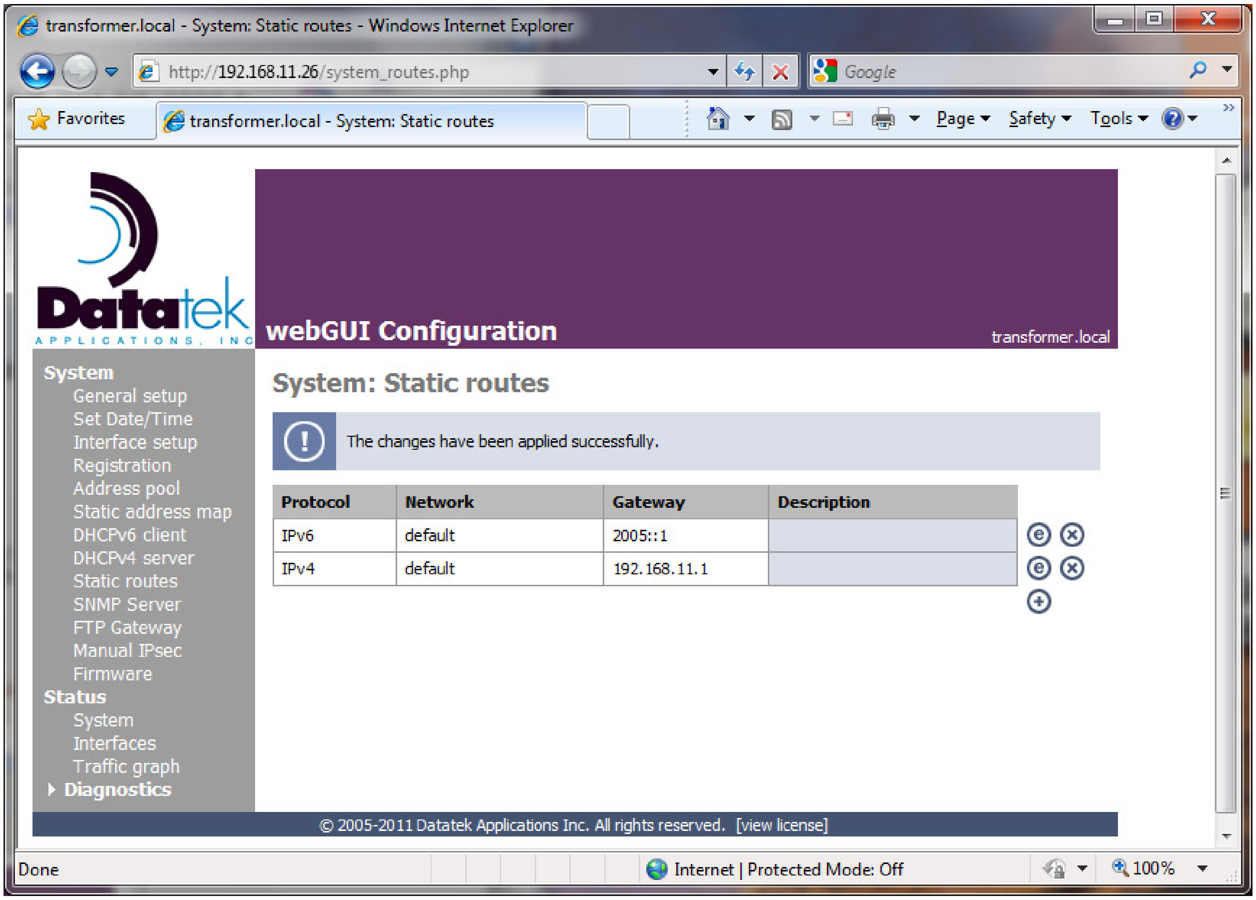
The primary and secondary DNS addresses that are served to the legacy host are the addresses that were configured on the General Setup *form.*

⊕ Static Address assignment list

Select the ⊕ to add a specific client by MAC and IP address that the Transformer is to serve. All other clients are ignored. This is used in conjunction with the **Deny unknown clients** option.

Static routes

Figure 21. Static routes Screen shows how static routes can be added, edited or deleted. Both IPv4 and IPv6 networks can be configured.



System: Static routes

The changes have been applied successfully.

Protocol	Network	Gateway	Description
IPv6	default	2005::1	
IPv4	default	192.168.11.1	

Figure 21. Static routes Screen

8.10 SNMP Server

An enterprise MIB has been implemented on the Transformer that allows viewing translation-specific configuration and statistics. Included with the Transformer's SNMP implementation is a standard MIB file named DATATEK.TXT that allows reading out many different system parameters (IP addresses, performance measures, etc.) and their descriptions. An NMS that supports custom MIBs should be able to display the list of available parameters. That MIB does not support changing or clearing any parameters.

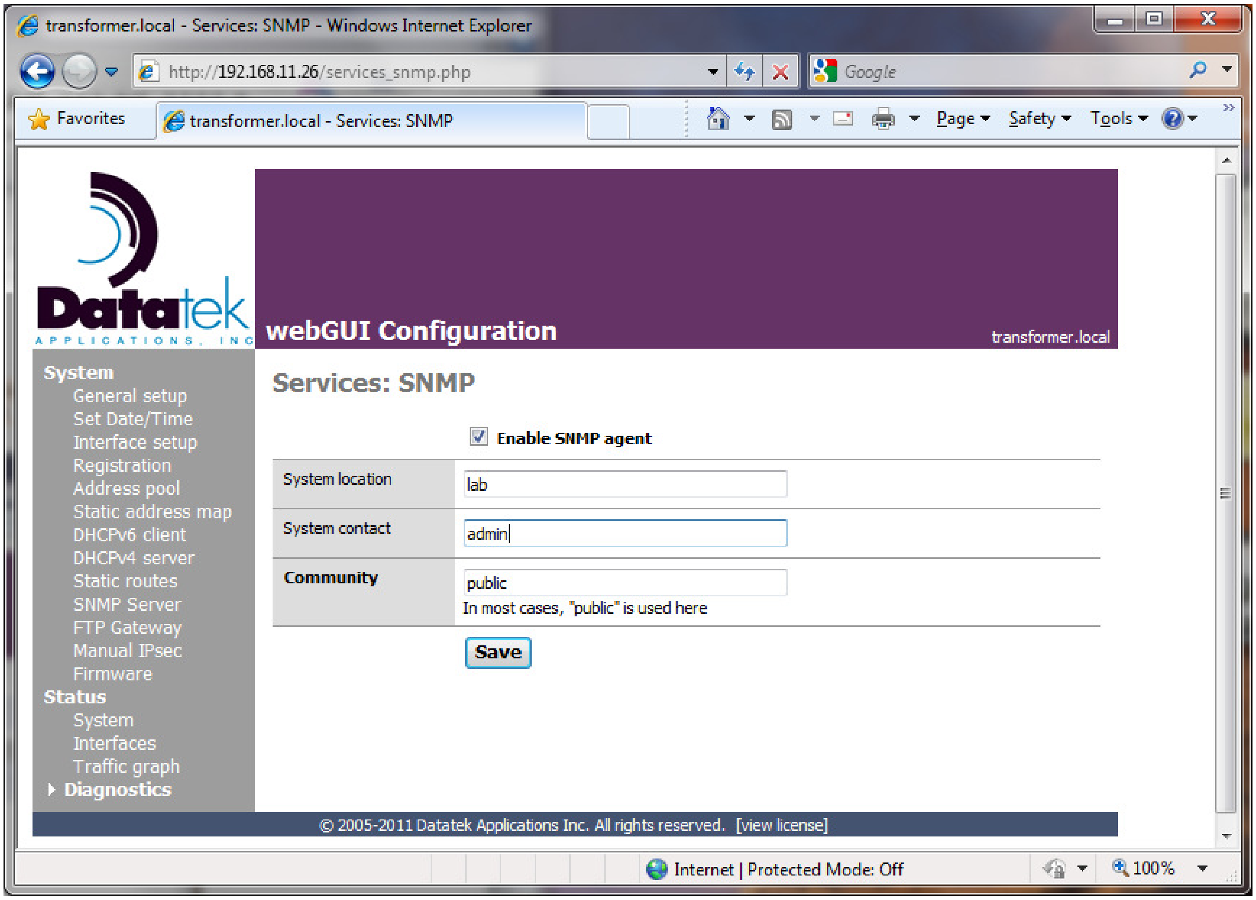
This DATATEK.TXT file does not get put on the Transformer. Instead, it is loaded on a customer's NMS to merge with all the other MIB descriptors it is expected to find on systems with SNMP agents. The NMS can use information in this file to direct formatted display of data and some descriptive text. Without this file, an NMS can only display raw data and does not display tables well.

Besides this MIB, there are other MIBs supported on the Transformer. Hundreds of data items are supported. See e.g. mibII.

To generate a list, set up an NMS that supports loading additional MIBS. Tell it where to find the DATATEK.txt file. Then have the NMS walk the system using a command-line snmp utility to display everything. It has a list of standard MIBs (in /etc somewhere) and supports adding extension MIBs in the user's $HOME/.snmp/mibs directory.

Some of the SNMP objects included in the Transformer's MIB are: IPv4 and IPv6 addresses, number of IPv4 packets mapped from host to network and vice versa, number of IPv4 packets passed from host to network and vice versa, number of packets dropped from host, number of IPv4 packets translated to IPv6 and vice versa, number of IPv6 packets translated to IPv4, number of IPv6 packets not translated, number of IPv4 and IPv6 packets dropped, number of packets with untranslatable protocol, number of packets with bad ICMP format, etc.

Figure 22. SNMP Server Screen shows a checkbox which the user can select to enable the SNMP agent. It also has descriptor fields to identify the location of the Transformer, system contact information and the community the Transformer is part of.



Services: SNMP

☑ Enable SNMP agent

System location	lab
System contact	admin
Community	public In most cases, "public" is used here

Save

© 2005-2011 Datatek Applications Inc. All rights reserved. [view license]

Figure 22. SNMP Server Screen

8.11 FTP Gateway

FTP uses a command and response protocol over a connection from a client to a server established to a predefined TCP port. The FTP protocol is used to initiate file transfers and other data transfers over dynamically established connections.

When using the Transformer, an IPv4 host that uses FTP, either as a client or a server, is positioned on the v4 side of the Transformer, with the rest of the network on the other side. That host may need to continue using FTP, but now a layer of addressing and protocol transformation stands between that host and any remote host. The major problem is that the protocol requires exchanging address and protocol information, but the two sides have differing views of both the addressing and the protocol. To resolve that problem, the Transformer provides an "application layer gateway" (ALG) to provide the transformation that allows the two hosts to communicate.

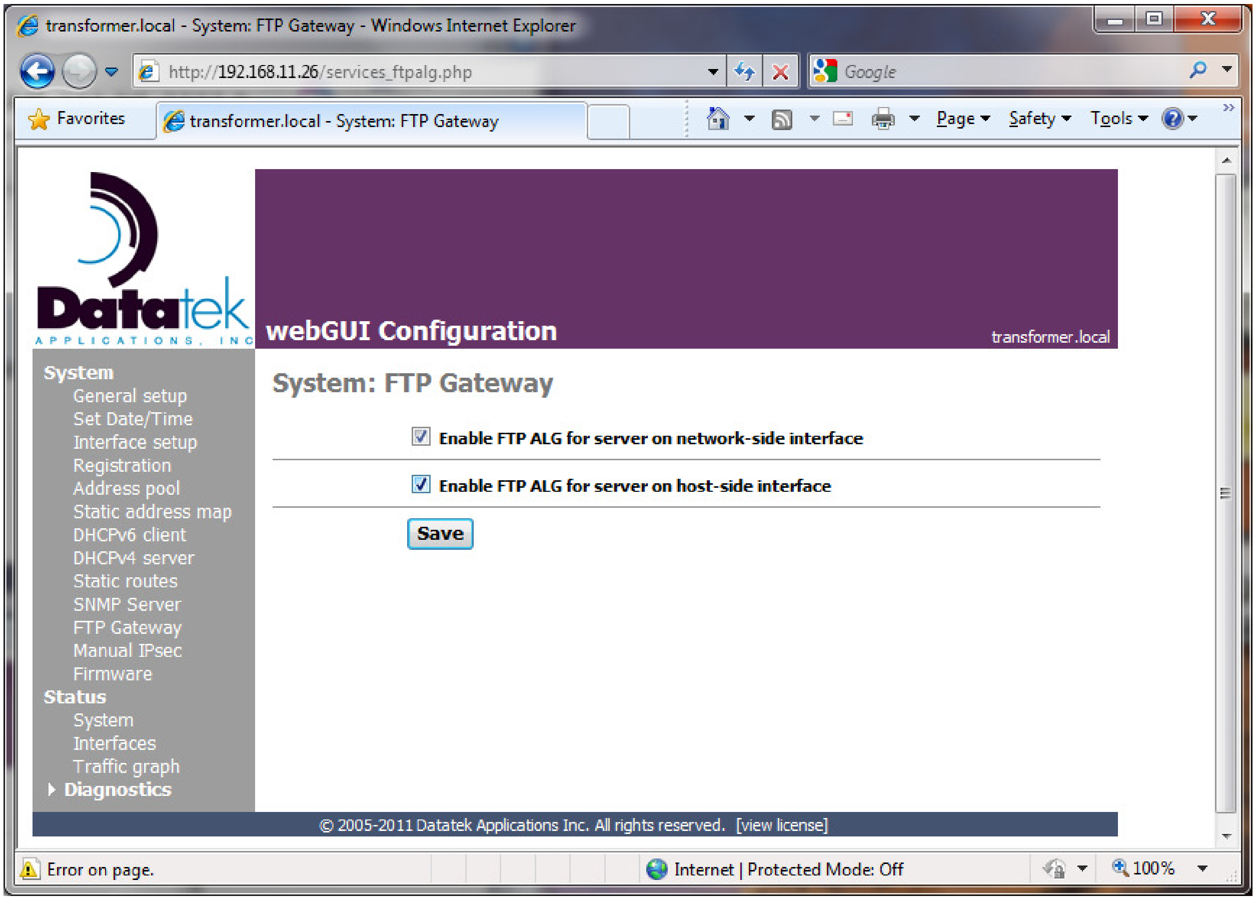
Figure 23. FTP Gateway Screen shows there are 2 choices that a user can select: to enable the FTP-ALG calling a host-side and/or network-side server on the standard FTP port. By checking one or both entries, the ALG is activated, which will perform the proper IPv4-IPv6 translation between the client and server. The variations covered by the FTP-ALG are:

Client on IPv4 host, IPv6 server on network

Client on IPv4 host, IPv4 server on network

IPv6 client on network, server on IPv4 host

IPv4 client on network, server on IPv4 host

- 

System: FTP Gateway

☑ Enable FTP ALG for server on network-side interface

☑ Enable FTP ALG for server on host-side interface

© 2005-2011 Datatek Applications Inc. All rights reserved. [view license]

Figure 23. FTP Gateway Screen

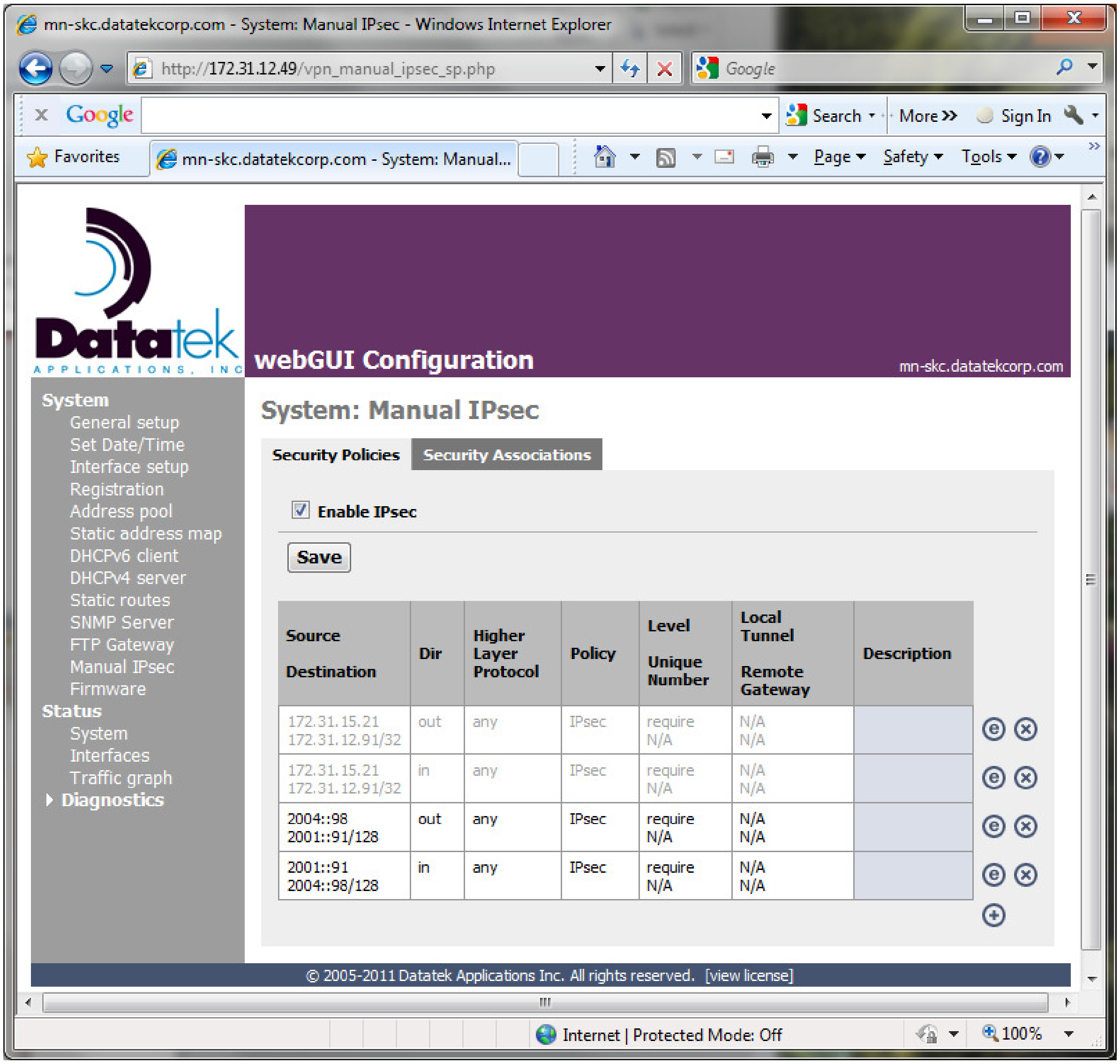
8.12 Manual IPsec

Figure 24. Manual IPsec Security Policies Screen and **Figure 25. Manual IPsec Security Associations Screen** display currently configured Security Policies (SPs) and Security Associations (SAs). Select the Security Policies tab to see the SPs displayed on the screen. Select the Security Associations tab to see the SAs displayed on the screen. The following control buttons are at the end of each row:

⊕ Add a new configuration.

ⓔ Edit an existing configuration.

⊗ Delete an existing configuration.



System: Manual IPsec

Security Policies | Security Associations

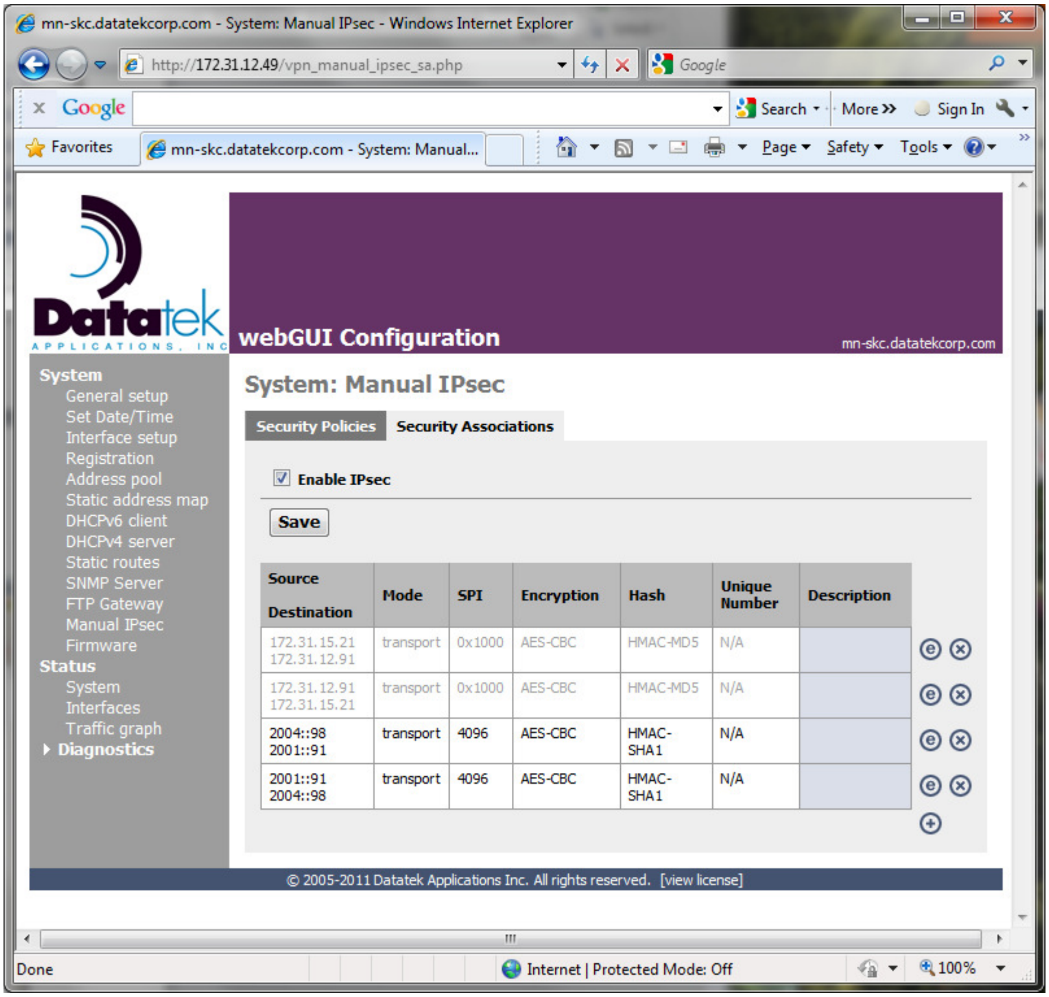
☑ Enable IPsec

Save

Source Destination	Dir	Higher Layer Protocol	Policy	Level Unique Number	Local Tunnel Remote Gateway	Description	
172.31.15.21 172.31.12.91/32	out	any	IPsec	require N/A	N/A N/A		ⓔ ⊗
172.31.15.21 172.31.12.91/32	in	any	IPsec	require N/A	N/A N/A		ⓔ ⊗
2004::98 2001::91/128	out	any	IPsec	require N/A	N/A N/A		ⓔ ⊗
2001::91 2004::98/128	in	any	IPsec	require N/A	N/A N/A		ⓔ ⊗
							⊕

© 2005-2011 Datatek Applications Inc. All rights reserved. [view license]

Figure 24. Manual IPsec Security Policies Screen



System: Manual IPsec

☑ Enable IPsec

Source Destination	Mode	SPI	Encryption	Hash	Unique Number	Description
172.31.15.21 172.31.12.91	transport	0x1000	AES-CBC	HMAC-MD5	N/A	
172.31.12.91 172.31.15.21	transport	0x1000	AES-CBC	HMAC-MD5	N/A	
2004::98 2001::91	transport	4096	AES-CBC	HMAC-SHA1	N/A	
2001::91 2004::98	transport	4096	AES-CBC	HMAC-SHA1	N/A	

Figure 25. Manual IPsec Security Associations Screen

Enable IPsec

This check box is selected to apply any SP or SA configurations that may be in the configuration database to the SP and SA databases in memory. Uncheck this box for a quick way to disable all IPsec on the Transformer without having to delete any SP or SA configurations from the flash.

Note

*If you intend to use IPsec, **Enable IPsec** must be selected.*

Apply Changes

This control button appears when an SP or SA has been changed through the e, ⊗, or + buttons. Click **Apply Changes** to update the SP and SA databases in memory so that the changes will take effect. The new IPsec changes will not be applied until you select **Apply Changes**.

8.13 Manual IPsec: Security Policy

Manual IPsec -> Security Policies -> ⓔ

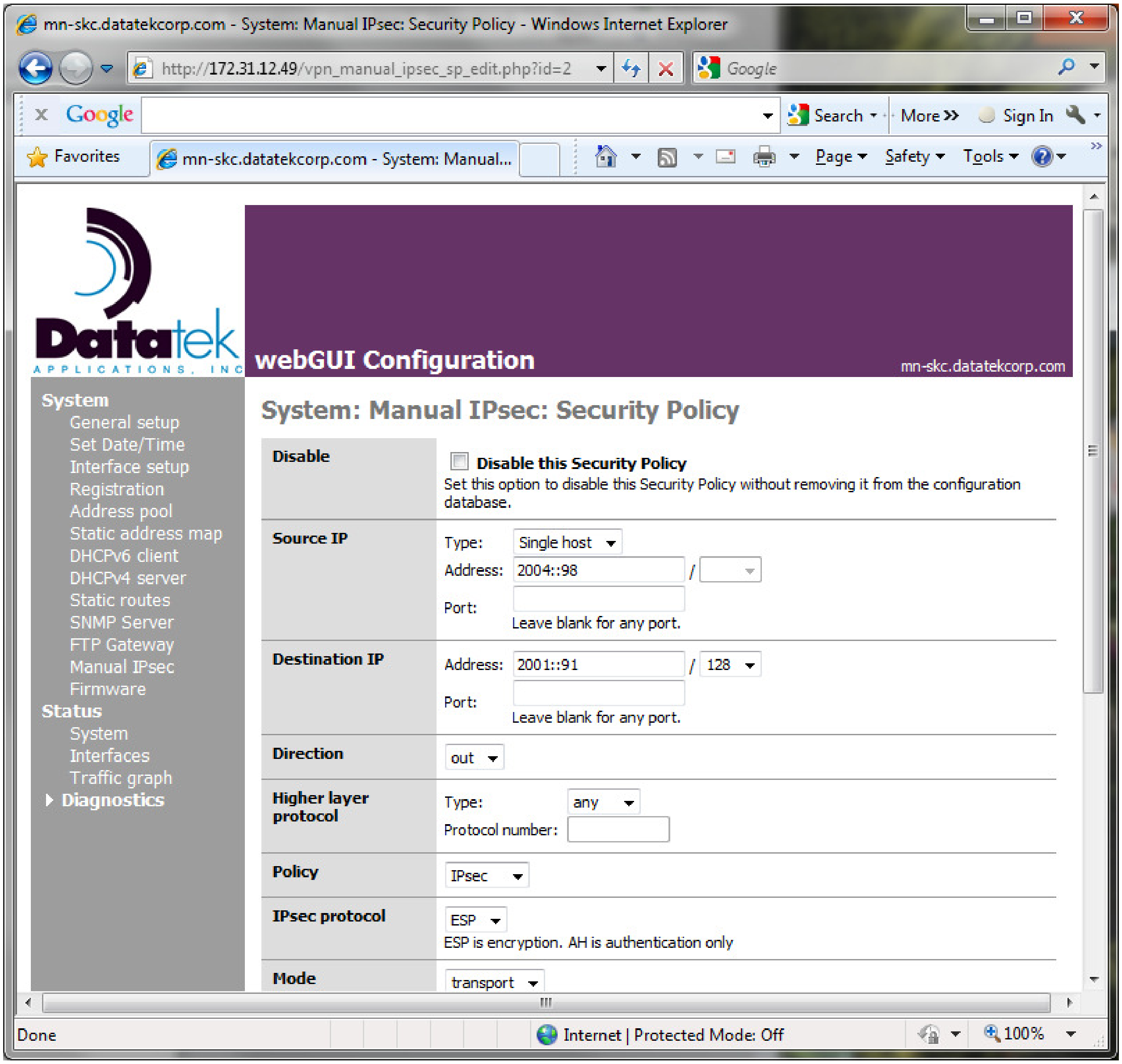
Manual IPsec -> Security Policies -> ⊕

Figure 26. Manual IPsec: Security Policy Edit Screen and **Figure 27. Manual IPsec : Security Policy Edit Screen continued** are used to add a new Security Policy (SP) or edit an existing SP. Selection parameters specified on this form are matched against fields in the IP header and upper layer protocol header of IP packets. Examples of some of these selection parameters are:

- Direction
- Source IP address and port
- Destination IP address and port
- Higher layer protocol

If a packet matches the specified parameters above, the specified **policy** is carried out. Use the following buttons to:

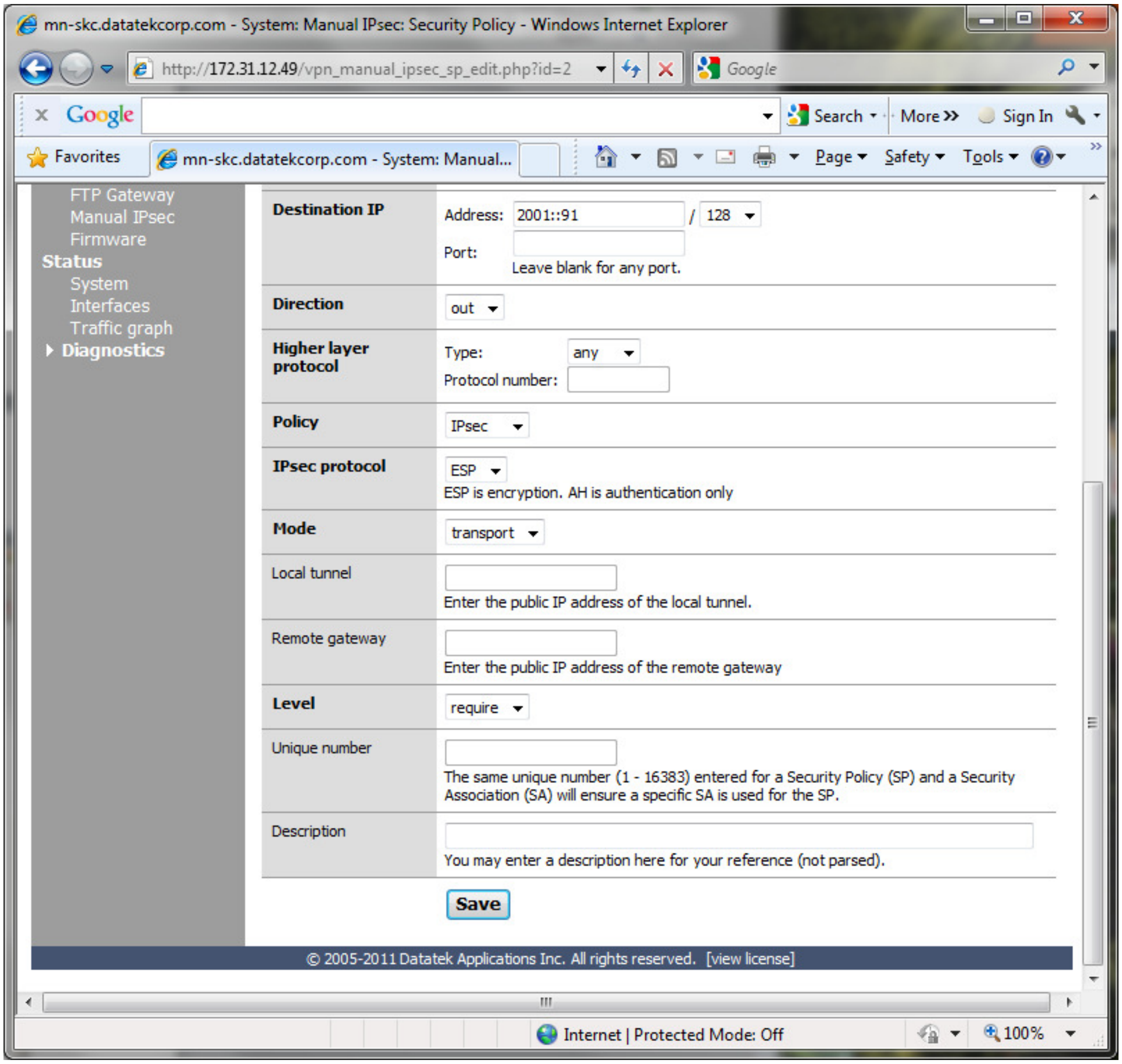
⊕ Add a new configuration.
ⓔ Edit an existing configuration.
⊗ Delete an existing configuration.



System: Manual IPsec: Security Policy

Disable	□ **Disable this Security Policy** Set this option to disable this Security Policy without removing it from the configuration database.
Source IP	Type: Single host Address: 2004::98 / Port: Leave blank for any port.
Destination IP	Address: 2001::91 / 128 Port: Leave blank for any port.
Direction	out
Higher layer protocol	Type: any Protocol number:
Policy	IPsec
IPsec protocol	ESP ESP is encryption. AH is authentication only
Mode	transport

Figure 26. Manual IPsec: Security Policy Edit Screen


mn-skc.datatekcorp.com - System: Manual IPsec: Security Policy - Windows Internet Explorer
http://172.31.12.49/vpn_manual_ipsec_sp_edit.php?id=2
Google
Search
More »
Sign In
Favorites
mn-skc.datatekcorp.com - System: Manual...
Page
Safety
Tools
FTP Gateway
Manual IPsec
Firmware
Status
System
Interfaces
Traffic graph
Diagnostics
Internet | Protected Mode: Off
100%

Destination IP	Address: 2001::91 / 128 Port: Leave blank for any port.
Direction	out
Higher layer protocol	Type: any Protocol number:
Policy	IPsec
IPsec protocol	ESP ESP is encryption. AH is authentication only
Mode	transport
Local tunnel	Enter the public IP address of the local tunnel.
Remote gateway	Enter the public IP address of the remote gateway
Level	require
Unique number	The same unique number (1 - 16383) entered for a Security Policy (SP) and a Security Association (SA) will ensure a specific SA is used for the SP.
Description	You may enter a description here for your reference (not parsed).

Save

© 2005-2011 Datatek Applications Inc. All rights reserved. [view license]

Figure 27. Manual IPsec : Security Policy Edit Screen continued

Disable

This box is checked to disable the SP without deleting all its parameters from the configuration database.

Source IP

This is the source IP address of the SP. This field is comprised of an IP address and a port number. The IP address is matched against the source address in the IP header and the port number is matched against the port number in the higher layer protocol header. Leave the port field blank to allow any port number if the higher layer protocol does not support port numbers.

The type of address may be a single host or a network address. For a single host IPv6 address all 128 bits of the address are matched and for an IPv4 address, all 32 bits of the address are matched. A typical single host may be the IPv6 address of a legacy IPv4 host. For a network address, the number of subnet mask bits are selected from a pull-down menu. A network address may be the subnet on which the Transformer resides.

Destination IP

This is the destination IP address of the SP. This field is comprised of an IP address and a port number. The IP address is matched against the destination address in the IP header and the port number is matched against the port number in the higher layer protocol header. Leave the port field blank to allow any port number if the higher layer protocol does not support port numbers. The number of subnet mask bits is selected from a pull-down menu.

Direction

in specifies that the SP is matched against inbound packets while **out** specifies the SP is matched against outbound packets.

Inbound packets may be received from the network side or host side.
Outbound packets are either originated by the Transformer or forwarded by the Transformer. For example, a ping command initiated from the Transformer's console creates an outbound ICMP packet. Such a packet is matched against the parameters of an SP whose direction is *out*.

An example of an outbound packet that comes from forwarding is where packets are received from the legacy host, translated and then forwarded towards the network. Whenever, a packet is forwarded, it is considered to be in the outbound direction. Therefore, during the forwarding process, the parameters of an SP whose direction is *out* are matched against the packet being forwarded.

Higher Layer Protocol

IPsec allows an SP to match against the next higher layer protocol in the protocol stack. The commonly used higher layer protocols, **TCP**, **UDP**, **ICMP** are selected from the pull-down menu. To specify any other protocol, select **other** and enter the protocol number as it will appear in the IP packet's next header field. If the SP is to apply to all higher layer protocols, select **any**.

Policy

This is the action to take if the packet matches the selection criteria. The following actions are supported:

- **ipsec** - Authentication and/or encryption is to be performed.
- **discard** - The packet is to be discarded.
- **none** - Accept the packet without any processing.

IPsec Protocol

IPsec supports the Authentication Header (AH) protocol and the Encapsulating Security Payload (ESP) protocol. Select AH to provide authentication and integrity across the IP header, AH header and the IP payload. Select ESP to provide confidentiality across the IP payload. When ESP is selected, an Integrity Check Value (ICV) is always performed for heightened security. The ICV is computed over the ESP header Security Parameter Index (SPI) and Sequence Number, the IP payload and the ESP trailer (padding, padding length field and next header). Note that the IP header is excluded from the ICV computation.

Mode

IPsec supports two modes, tunnel mode and transport mode. In tunnel mode, an outer IP header comprised of the tunnel endpoints is pre-pended to the original packet before AH or ESP processing is performed on the entire original IP packet. Therefore, in tunnel mode, IPsec processing covers both the original IP header and the payload. In transport mode, ESP encryption mainly covers the IP payload and AH integrity covers both the IP header and the payload.

Local tunnel

This is the IP address of the local gateway or local tunnel endpoint that will appear in the outer IP header. In the outbound direction, this would be the tunnel source endpoint. In the inbound direction this would be the tunnel destination endpoint. This field is only active when the **Mode** is tunnel.

Remote Gateway

This is the IP address of the remote gateway or remote tunnel endpoint that will appear in the outer IP header. In the outbound direction, this would be the tunnel destination endpoint. In the inbound direction this would be the tunnel source endpoint. This field is only active when the **Mode** is tunnel.

Level

This specifies how the SA is to be regarded. **required** means an SA must exist or the packet will be discarded. **use** means an SA is not mandatory but if an SA exists it will be used. **unique** means apply a specific SA that uniquely corresponds to this SP. This one-to-one correspondence is established through the **unique** parameter. **Level** is only active if this SP's **Policy** is to perform **ipsec**.

Unique Number

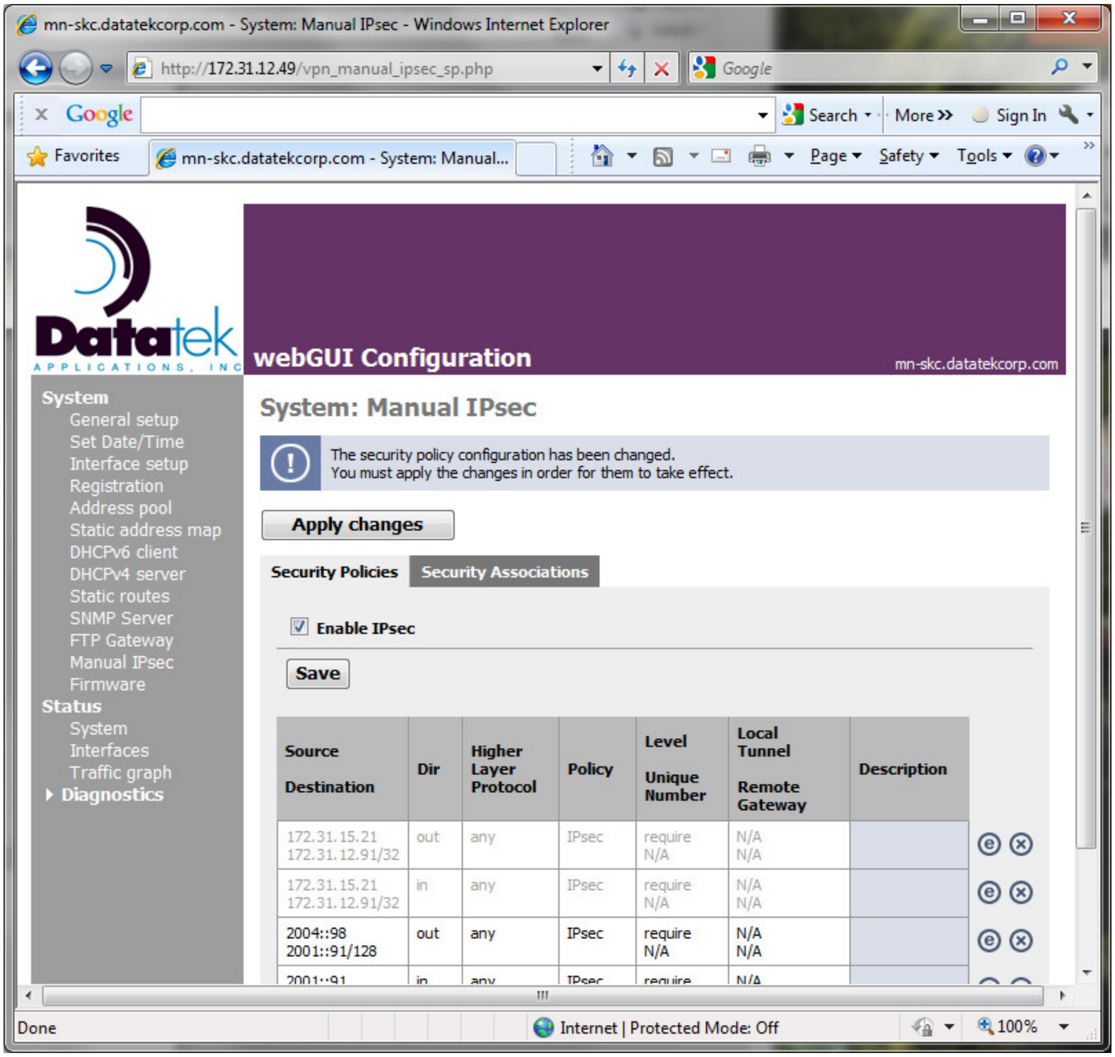
This is a number from 1 through 16,383 that is configured in the SP and the corresponding SA that is to be used for this SP.

Description

Enter up to 80 characters to describe this SP. This field is not processed but simply recorded as a comment for this SP.

Save

Click this button to write the parameters to the configuration database on the flash. Afterwards, the System: Manual IPsec screen will appear with an Apply Changes button at the top as shown in **Figure 28. Manual IPsec Security Policies Display after editing.** Click the Apply Changes button to update the SP and SA databases in memory.



System: Manual IPsec

The security policy configuration has been changed.
You must apply the changes in order for them to take effect.

☑ Enable IPsec

Source Destination	Dir	Higher Layer Protocol	Policy	Level Unique Number	Local Tunnel Remote Gateway	Description
172.31.15.21 172.31.12.91/32	out	any	IPsec	require N/A	N/A N/A	
172.31.15.21 172.31.12.91/32	in	any	IPsec	require N/A	N/A N/A	
2004::98 2001::91/128	out	any	IPsec	require N/A	N/A N/A	
2001::91	in	any	IPsec	require	N/A	

Figure 28. Manual IPsec Security Policies Display after editing

8.14 Manual IPsec: Security Associations

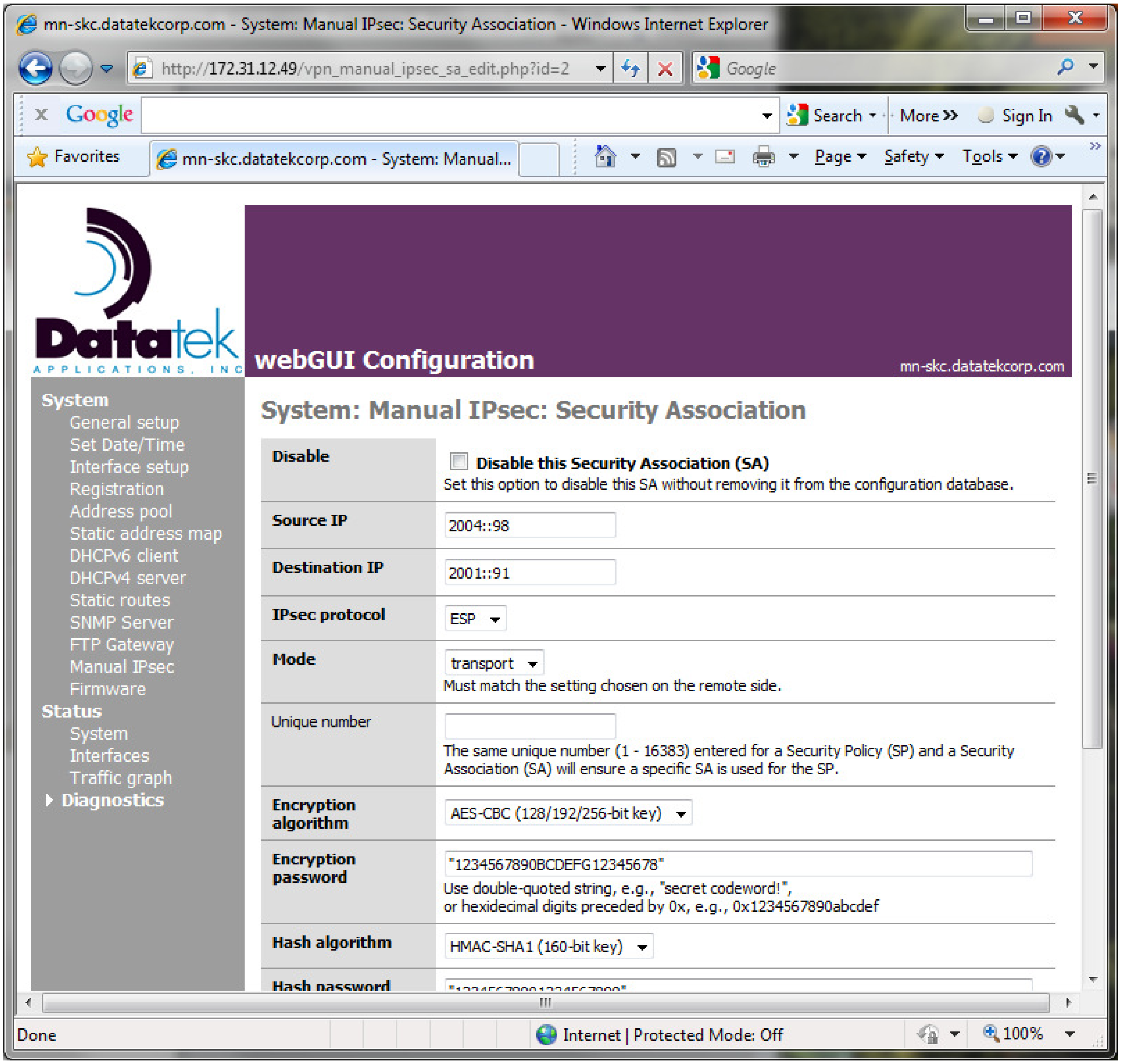
System -> Manual IPsec -> Security Associations -> ⓔ

System -> Manual IPsec -> Security Associations -> ⊕

Figure 29. Manual IPsec: Security Association Edit Screen is used to add a new Security Association (SA) or edit an existing SA. Parameters on this form specify how the packet is to be

encrypted and/or authenticated. The following parameters on this form are used to uniquely identify an SA and match it to a packet: These are some examples:

- Security Policy Index (SPI)
- Destination IP address and port
- IPsec protocol, ESP or AH



System: Manual IPsec: Security Association

Disable	☐ **Disable this Security Association (SA)** Set this option to disable this SA without removing it from the configuration database.
Source IP	2004::98
Destination IP	2001::91
IPsec protocol	ESP
Mode	transport Must match the setting chosen on the remote side.
Unique number	 The same unique number (1 - 16383) entered for a Security Policy (SP) and a Security Association (SA) will ensure a specific SA is used for the SP.
Encryption algorithm	AES-CBC (128/192/256-bit key)
Encryption password	"1234567890BCDEFG12345678" Use double-quoted string, e.g., "secret codeword!", or hexidecimal digits preceded by 0x, e.g., 0x1234567890abcdef
Hash algorithm	HMAC-SHA1 (160-bit key)
Hash password	"12345678901234567890"

Figure 29. Manual IPsec : Security Association Edit Screen

Disable

This box is checked to disable the SA without deleting all its parameters from the configuration database.

Source IP

This is the source IP address of the SA. The IP address is matched against the source address in the IP header.

Destination IP

This is the destination IP address of the SA. The IP address is matched against the destination address in the IP header. The destination IP address, in conjunction with the Security Parameter Index and the IPsec protocol, uniquely identify the SA.

IPsec Protocol

See the IPsec Protocol description in the section, Manual IPsec: Security Policy. The IPsec Protocol, in conjunction with the destination IP address and the Security Parameter Index uniquely identify the SA.

Mode

See the Mode description in the section, Manual IPsec: Security Policy. The Mode must match the setting chosen on the remote side.

Unique Number

This is the same number, from 1 through 16,383 that was configured in the SP. Configuring the same Unique Number for the SA and SP ensures this SA is used for the SP.

Encryption Algorithm

This is the encryption algorithm used to protect the IP payload. Each algorithm must use a key of a specific length.

Encryption Password

This is the key the encryption algorithm uses to provide confidentiality. The mandatory length of each key is determined by the encryption algorithm.

The encryption key can be entered as an ASCII character string in double quotes or as hexadecimal sequence starting with 0x. If the key is entered as an ASCII string, each character is treated as an 8-bit quantity. E.g. "12345678" is a 64 bit key, equivalent to 0x3132333435363738.

Encryption Algorithm	Key Length [bits]
des-cbc	64
3des-cbc	192
aes-cbc	128/192/256
aes-ctr	160/224/288

Warning

aes-ctr is not recommended for use with static keys. Only use aes-ctr if IKE (Internet Key Exchange) is used for establishing keys.

Hash Algorithm

This is the authentication algorithm used to calculate the authentication data field applied across the encrypted payload. Each algorithm must use a key of a specific length.

Hash Password

This password or key, is used by the authentication algorithm to provide authentication and integrity. The authentication key can be entered as an ASCII character string in double quotes or as hexadecimal sequence starting with 0x. If the key is entered as an ASCII string, each character is treated as an 8-bit quantity. E.g. "12345678" is a 64 bit key, equivalent to 0x3132333435363738.

Authentication Algorithm	Key Length [bits]
hmac-md5	128
hmac-sha1	160

Security Parameter Index (SPI)

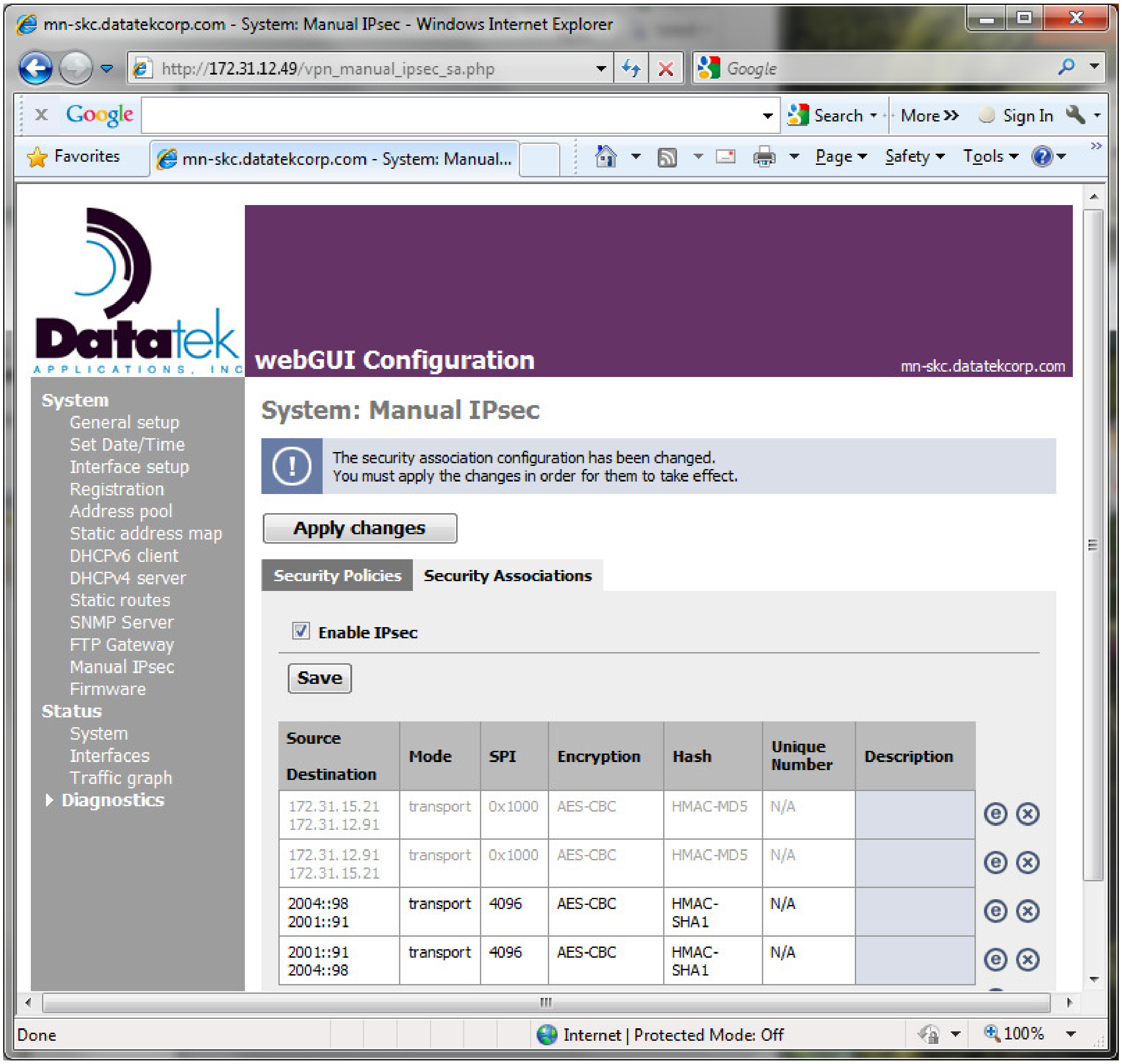
This is a 32 bit integer that is assigned to the SA. Valid values are 0x100 through 0xFFFFFFFF. The SPI, in conjunction with the destination IP address and the IPsec protocol, uniquely identify the SA.

Description

Enter up to 80 characters to describe this SA. This field is not processed but simply recorded as a comment for this SA.

Save

Click this button to write the parameters to the configuration database on the flash. Afterwards, the System: Manual IPsec screen will appear with an Apply Changes button at the top as shown in **Figure 30. Manual IPsec Security Associations Screen after editing** Click the Apply Changes button to update the SP and SA databases in memory.



System: Manual IPsec

The security association configuration has been changed.
You must apply the changes in order for them to take effect.

☑ Enable IPsec

Source Destination	Mode	SPI	Encryption	Hash	Unique Number	Description
172.31.15.21 172.31.12.91	transport	0x1000	AES-CBC	HMAC-MD5	N/A	
172.31.12.91 172.31.15.21	transport	0x1000	AES-CBC	HMAC-MD5	N/A	
2004::98 2001::91	transport	4096	AES-CBC	HMAC-SHA1	N/A	
2001::91 2004::98	transport	4096	AES-CBC	HMAC-SHA1	N/A	

Figure 30. Manual IPsec Security Associations Screen after editing

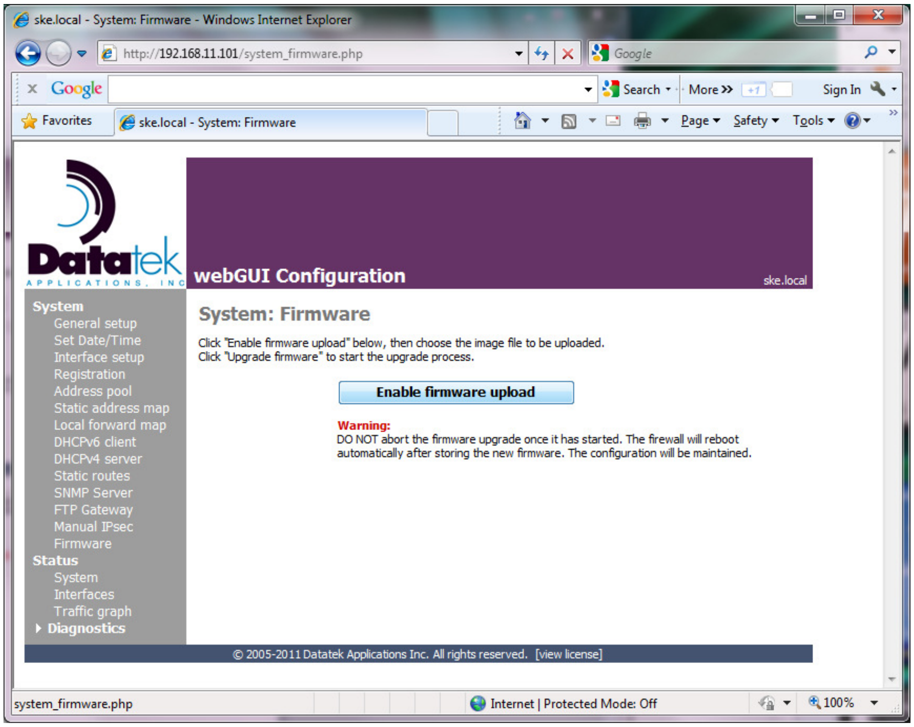
8.15 Firmware

Upgrading new firmware

New firmware upgrades may be obtained in several ways: FTP, email and distribution on CD-ROM. Datatek will alert all users via email and on its website that a new upgrade is available.

Datatek maintains a secure FTP site on its corporate website, so users can download it to their servers directly. If the user cannot use FTP for downloading purposes, email is an option. Contact Datatek support and the firmware image will be emailed, where it can be loaded on the user's server. Due to the size of the firmware upgrade, email may not be practical for some customers with a size limit on their email. A third option is to deliver the firmware upgrade on a CD, which will contain a Readme file and the firmware image. The user can then follow the Readme instructions for installing the upgrade from the CD itself or after loading the image on the server. Contact Datatek support for this option.

To load the new firmware upgrade on the Transformer, select the **Firmware** button from the left-hand menu items. On the Firmware screen, shown in **Figure 31. Firmware screen,** click the '**Enable Firmware upload**' button. Browse for the file, then click the '**Upgrade Firmware**' button to start the Transformer firmware upgrade process. A message will be displayed at the bottom of the Firmware screen, **"The firmware is now being installed. The Transformer will reboot automatically"**. Wait 2 to 3 minutes for the Transformer to finish the upgrade and reboot. **Do not power off the Transformer during the firmware upgrade process!** You will know when the reboot has finished if the Transformer responds to a click on any of the left-hand menu items.



System: Firmware

Click "Enable firmware upload" below, then choose the image file to be uploaded.
Click "Upgrade firmware" to start the upgrade process.

Warning:
DO NOT abort the firmware upgrade once it has started. The firewall will reboot automatically after storing the new firmware. The configuration will be maintained.

© 2005-2011 Datatek Applications Inc. All rights reserved. [view license]

Figure 31. Firmware screen

9 Web Graphical User Interface (webGUI) Status

The following forms are used for displaying the status of the Transformer, such as general system information, interfaces and traffic.

9.1 System information

Figure 32. System information Screen displays general system information about the Transformer.

Name

This is the name of the Transformer that is formed with the **Hostname** and **Domain** fields from the **General setup** screen.

Version

This is the image the Transformer is running. The version, filename and its date and time are displayed.

Platform

This field displays the Transformer hardware version.

Uptime

This is number of hours and minutes since the Transformer was last booted.

Last config change

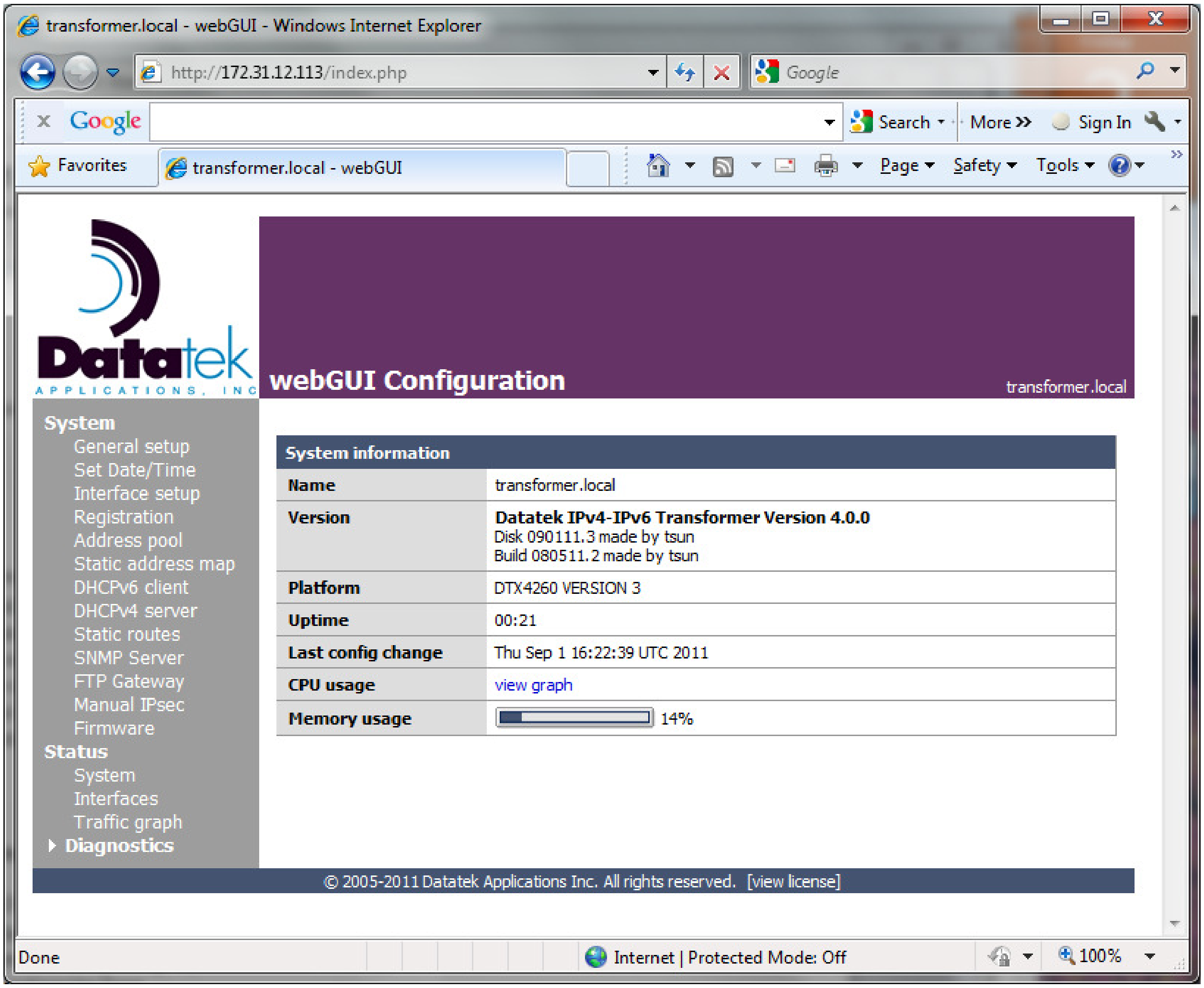
This dates the last time the database was saved.

CPU usage

Figure 33. CPU usage Screen. is a graph that tracks CPU usage, by clicking 'VIEW GRAPH' link.

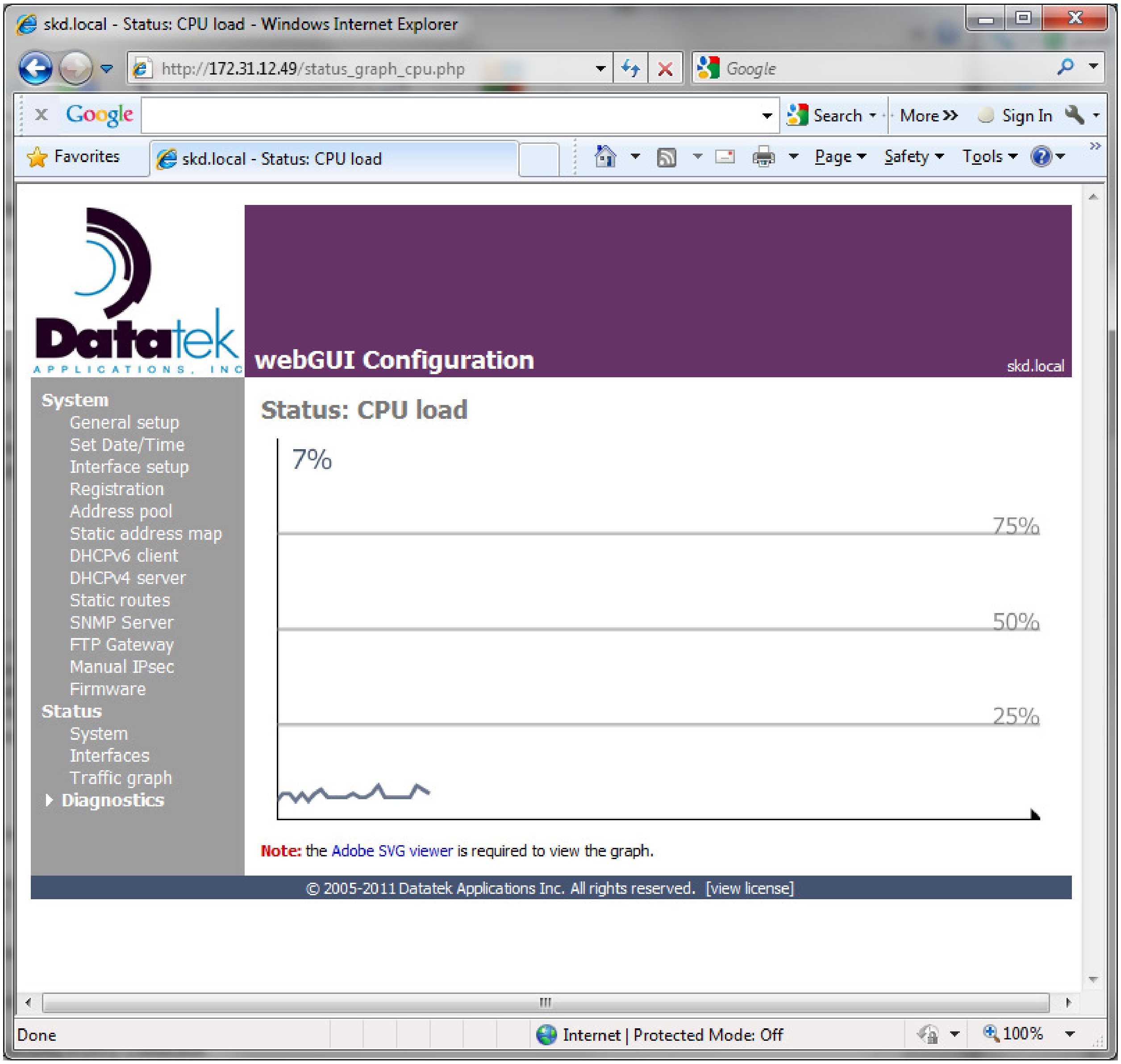
Memory usage

This is a bar graph that dynamically tracks memory usage.



System information	
Name	transformer.local
Version	Datatek IPv4-IPv6 Transformer Version 4.0.0 Disk 090111.3 made by tsun Build 080511.2 made by tsun
Platform	DTX4260 VERSION 3
Uptime	00:21
Last config change	Thu Sep 1 16:22:39 UTC 2011
CPU usage	view graph
Memory usage	14%

Figure 32. System information Screen



Status: CPU load

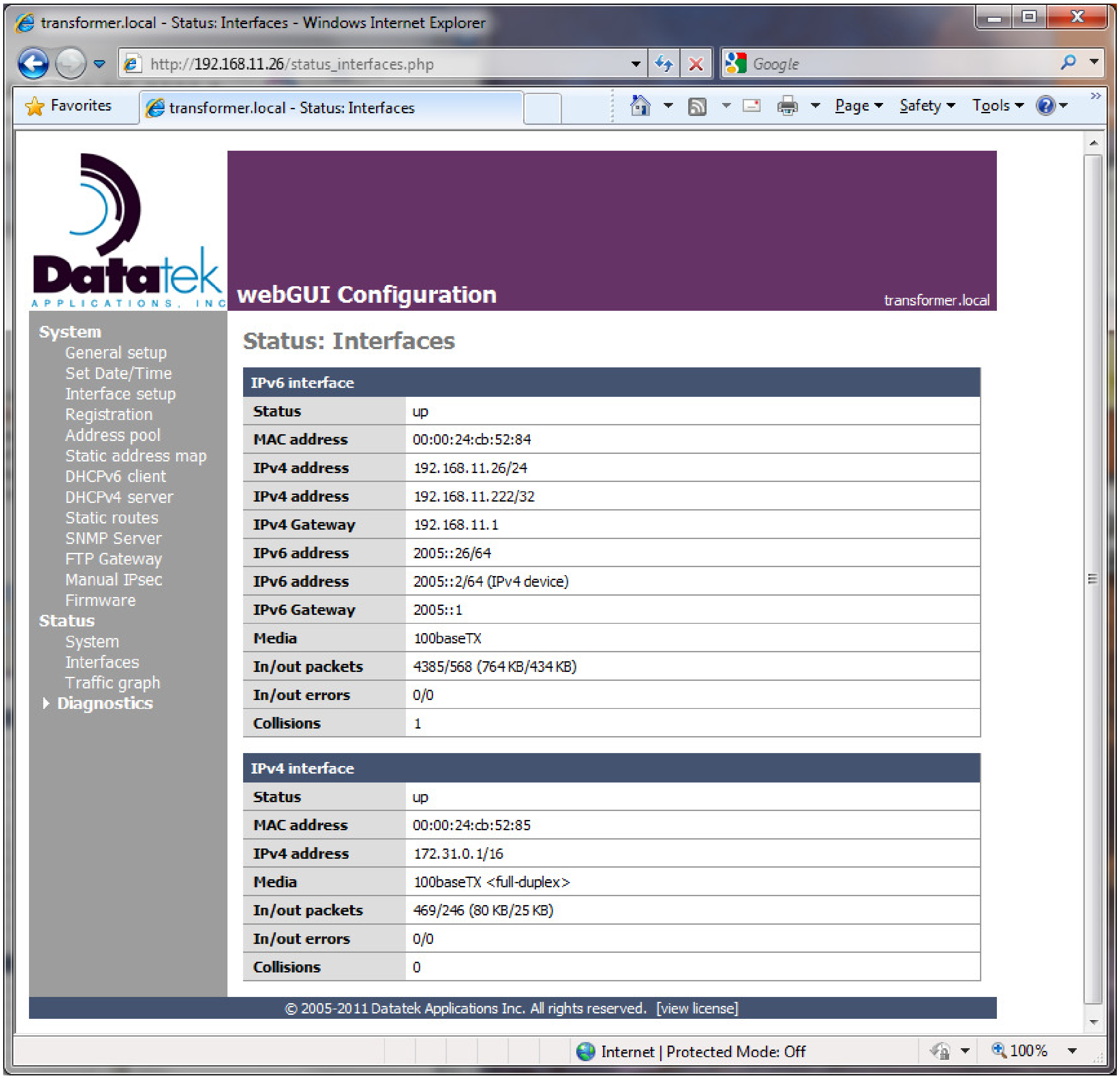
Note: the Adobe SVG viewer is required to view the graph.

© 2005-2011 Datatek Applications Inc. All rights reserved. [view license]

Figure 33. CPU usage Screen.

9.2 Interfaces

Figure 34. Interfaces Screen displays the up/down status of the link and the addresses configured on the IPv4 and IPv6 interfaces. On the IPv6 interface there are multiple addresses configured. Addresses associated with the IPv4 device are indicated with (IPv4 device). The IPv6 interface addresses include the link local address of the IPv4 device, the IPv6 address that is mapped to an IPv4 device and the foreign IPv6 care-of addresses. Other IPv6 addresses include the address of the IPv6/Network interface.



Status: Interfaces

IPv6 interface	
Status	up
MAC address	00:00:24:cb:52:84
IPv4 address	192.168.11.26/24
IPv4 address	192.168.11.222/32
IPv4 Gateway	192.168.11.1
IPv6 address	2005::26/64
IPv6 address	2005::2/64 (IPv4 device)
IPv6 Gateway	2005::1
Media	100baseTX
In/out packets	4385/568 (764 KB/434 KB)
In/out errors	0/0
Collisions	1

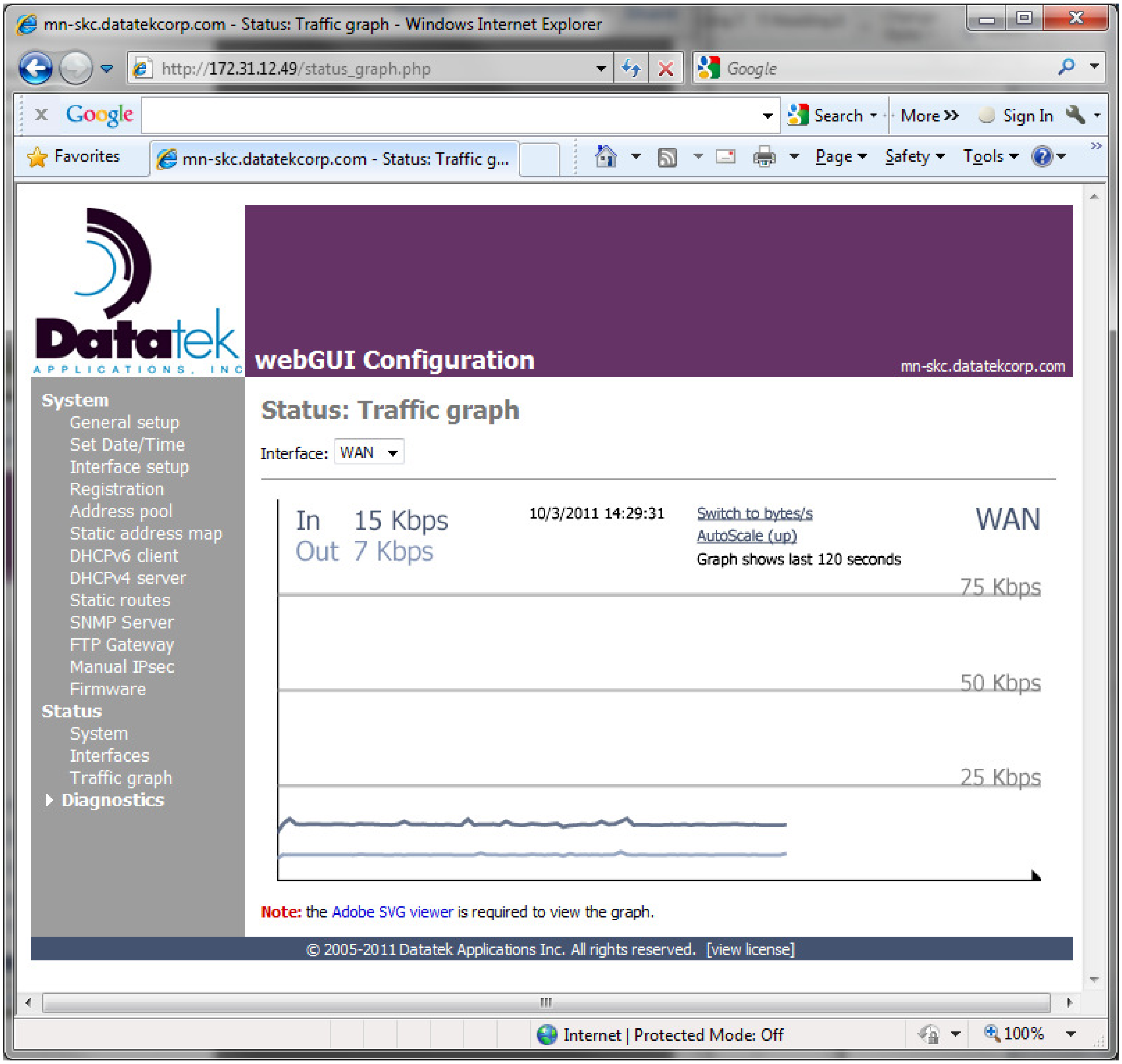
IPv4 interface	
Status	up
MAC address	00:00:24:cb:52:85
IPv4 address	172.31.0.1/16
Media	100baseTX <full-duplex>
In/out packets	469/246 (80 KB/25 KB)
In/out errors	0/0
Collisions	0

© 2005-2011 Datatek Applications Inc. All rights reserved. [view license]

Figure 34. Interfaces Screen

9.3 Traffic graph

Figure 35. Traffic graph Screen displays incoming and outgoing traffic for both the IPv4 (LAN) and IPv6 (WAN) interfaces.



Status: Traffic graph

Interface: WAN

In 15 Kbps
Out 7 Kbps

10/3/2011 14:29:31

Switch to bytes/s
AutoScale (up)
Graph shows last 120 seconds

WAN

Note: the Adobe SVG viewer is required to view the graph.

© 2005-2011 Datatek Applications Inc. All rights reserved. [view license]

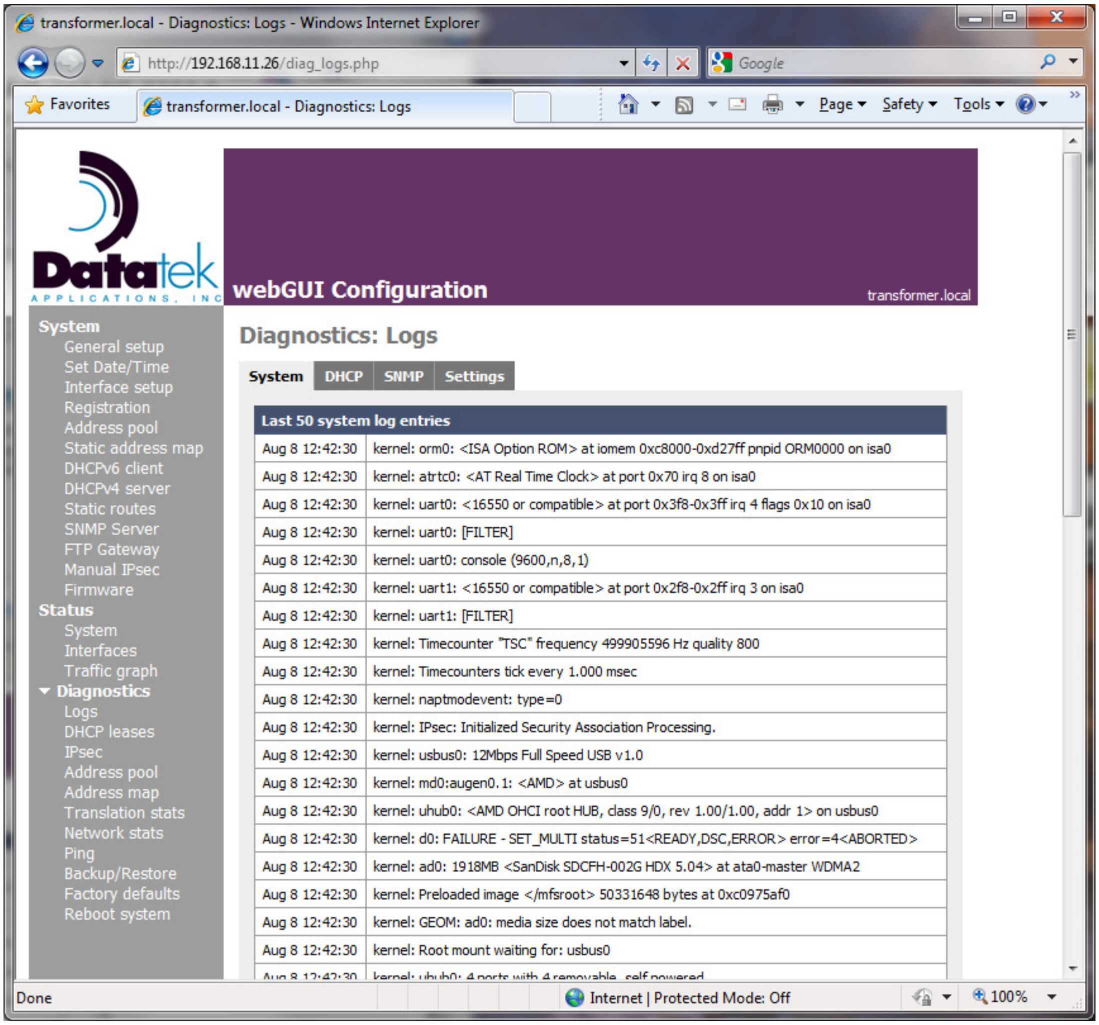
Figure 35. Traffic graph Screen

10 Web Graphical User Interface (webGUI) Diagnostics

The following forms are used for the maintenance and debugging of the Transformer.

10.1 Logs

Figure 36. Logs Screen displays the system log.

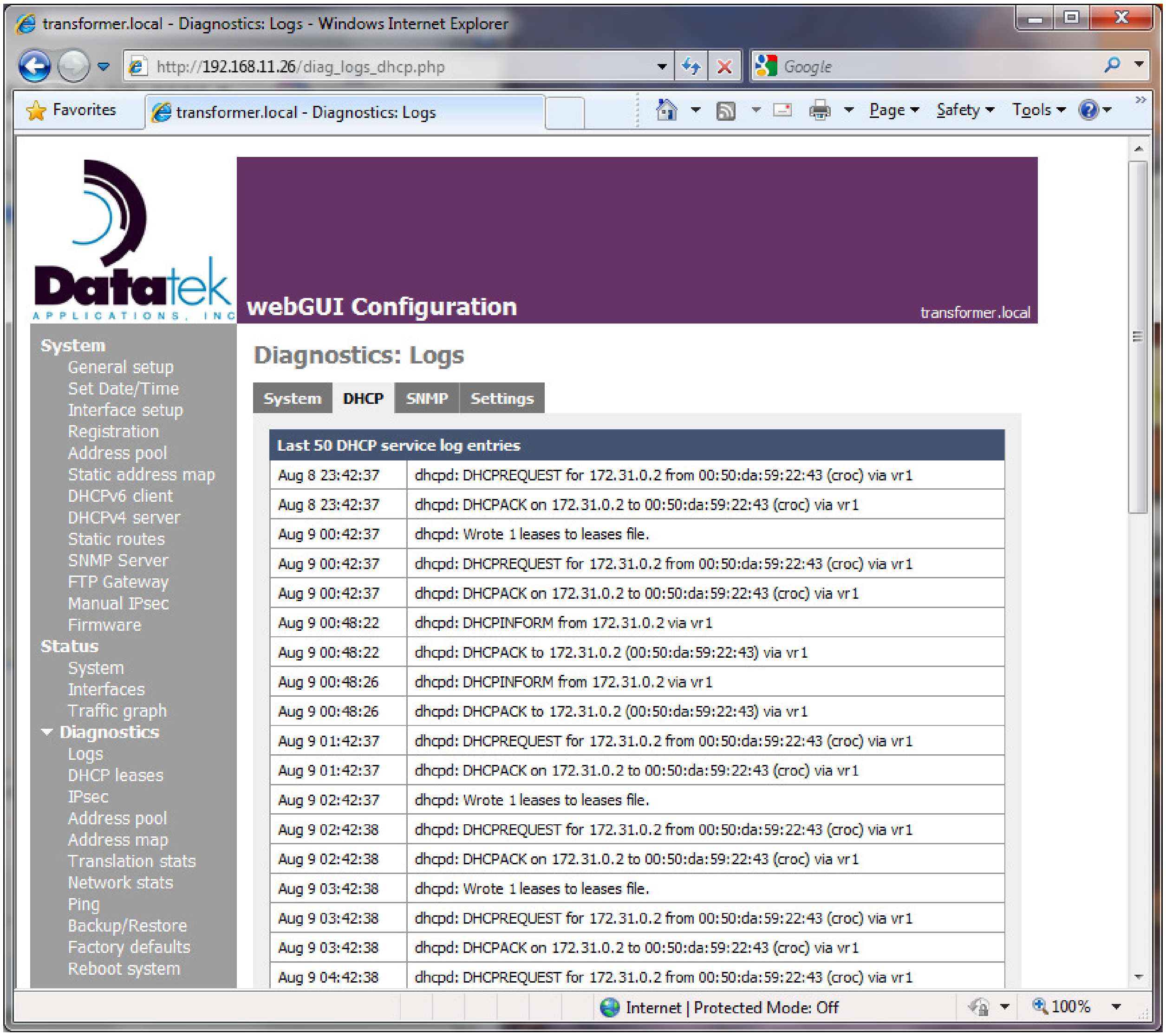


Last 50 system log entries	
Aug 8 12:42:30	kernel: orm0: <ISA Option ROM> at iomem 0xc8000-0xd27ff pnpid ORM0000 on isa0
Aug 8 12:42:30	kernel: atrtc0: <AT Real Time Clock> at port 0x70 irq 8 on isa0
Aug 8 12:42:30	kernel: uart0: <16550 or compatible> at port 0x3f8-0x3ff irq 4 flags 0x10 on isa0
Aug 8 12:42:30	kernel: uart0: [FILTER]
Aug 8 12:42:30	kernel: uart0: console (9600,n,8,1)
Aug 8 12:42:30	kernel: uart1: <16550 or compatible> at port 0x2f8-0x2ff irq 3 on isa0
Aug 8 12:42:30	kernel: uart1: [FILTER]
Aug 8 12:42:30	kernel: Timecounter "TSC" frequency 499905596 Hz quality 800
Aug 8 12:42:30	kernel: Timecounters tick every 1.000 msec
Aug 8 12:42:30	kernel: naptmodevent: type=0
Aug 8 12:42:30	kernel: IPsec: Initialized Security Association Processing.
Aug 8 12:42:30	kernel: usbus0: 12Mbps Full Speed USB v1.0
Aug 8 12:42:30	kernel: md0:augen0.1: <AMD> at usbus0
Aug 8 12:42:30	kernel: uhub0: <AMD OHCI root HUB, class 9/0, rev 1.00/1.00, addr 1> on usbus0
Aug 8 12:42:30	kernel: d0: FAILURE - SET_MULTI status=51<READY,DSC,ERROR> error=4<ABORTED>
Aug 8 12:42:30	kernel: ad0: 1918MB <SanDisk SDCFH-002G HDX 5.04> at ata0-master WDMA2
Aug 8 12:42:30	kernel: Preloaded image </mfsroot> 50331648 bytes at 0xc0975af0
Aug 8 12:42:30	kernel: GEOM: ad0: media size does not match label.
Aug 8 12:42:30	kernel: Root mount waiting for: usbus0
Aug 8 12:42:30	kernel: uhub0: 4 ports with 4 removable, self powered

Figure 36. Logs Screen

10.2 DHCP leases

Figure 37. DHCP leases Screen displays the status of current or past DHCP leases that are owned by the Transformer. It will not display any leases for locally forwarded IPv4 endpoints, however.



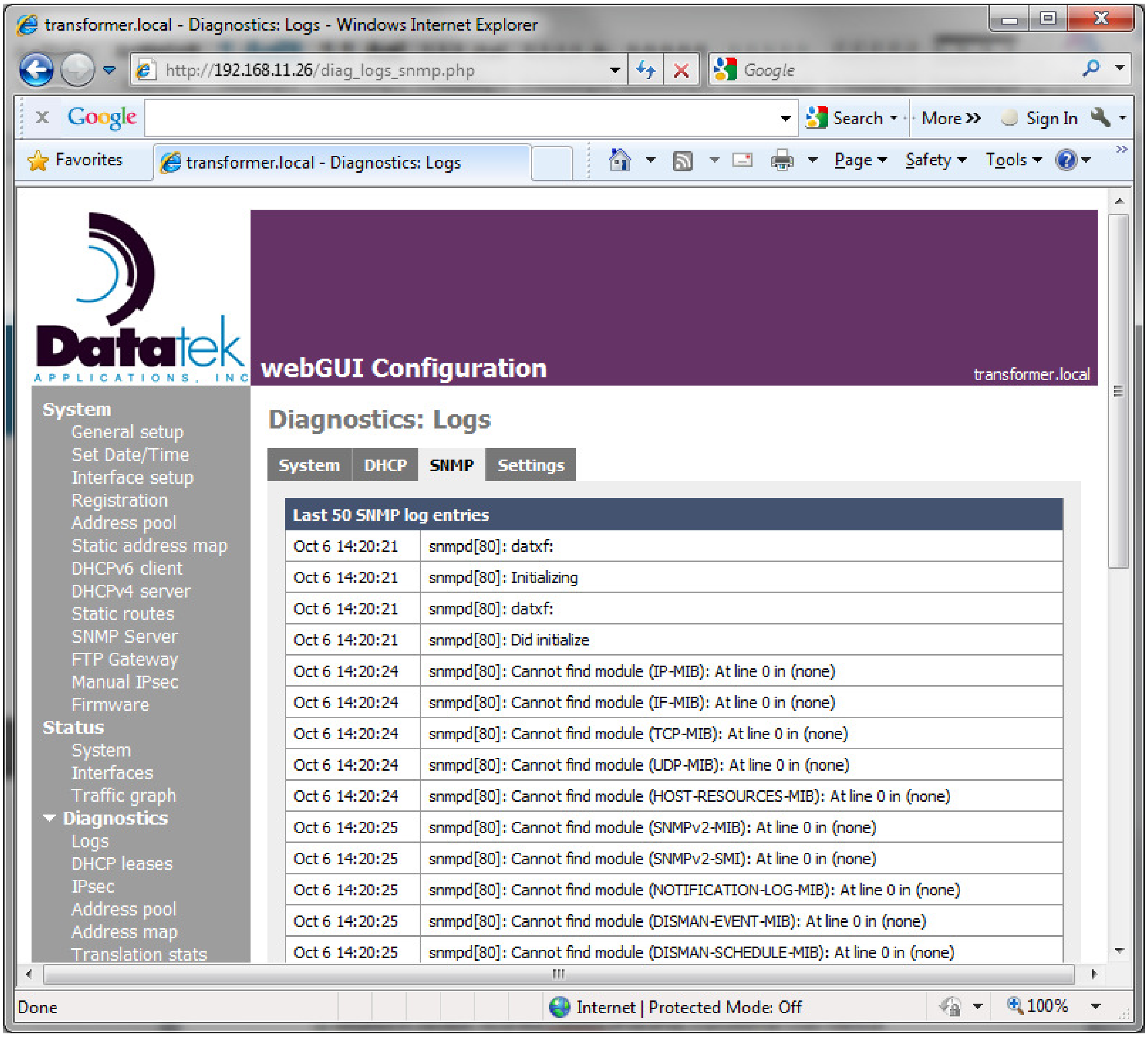
Last 50 DHCP service log entries

Aug 8 23:42:37	dhcpd: DHCPREQUEST for 172.31.0.2 from 00:50:da:59:22:43 (croc) via vr1
Aug 8 23:42:37	dhcpd: DHCPACK on 172.31.0.2 to 00:50:da:59:22:43 (croc) via vr1
Aug 9 00:42:37	dhcpd: Wrote 1 leases to leases file.
Aug 9 00:42:37	dhcpd: DHCPREQUEST for 172.31.0.2 from 00:50:da:59:22:43 (croc) via vr1
Aug 9 00:42:37	dhcpd: DHCPACK on 172.31.0.2 to 00:50:da:59:22:43 (croc) via vr1
Aug 9 00:48:22	dhcpd: DHCPINFORM from 172.31.0.2 via vr1
Aug 9 00:48:22	dhcpd: DHCPACK to 172.31.0.2 (00:50:da:59:22:43) via vr1
Aug 9 00:48:26	dhcpd: DHCPINFORM from 172.31.0.2 via vr1
Aug 9 00:48:26	dhcpd: DHCPACK to 172.31.0.2 (00:50:da:59:22:43) via vr1
Aug 9 01:42:37	dhcpd: DHCPREQUEST for 172.31.0.2 from 00:50:da:59:22:43 (croc) via vr1
Aug 9 01:42:37	dhcpd: DHCPACK on 172.31.0.2 to 00:50:da:59:22:43 (croc) via vr1
Aug 9 02:42:37	dhcpd: Wrote 1 leases to leases file.
Aug 9 02:42:38	dhcpd: DHCPREQUEST for 172.31.0.2 from 00:50:da:59:22:43 (croc) via vr1
Aug 9 02:42:38	dhcpd: DHCPACK on 172.31.0.2 to 00:50:da:59:22:43 (croc) via vr1
Aug 9 03:42:38	dhcpd: Wrote 1 leases to leases file.
Aug 9 03:42:38	dhcpd: DHCPREQUEST for 172.31.0.2 from 00:50:da:59:22:43 (croc) via vr1
Aug 9 03:42:38	dhcpd: DHCPACK on 172.31.0.2 to 00:50:da:59:22:43 (croc) via vr1
Aug 9 04:42:38	dhcpd: DHCPREQUEST for 172.31.0.2 from 00:50:da:59:22:43 (croc) via vr1

Figure 37. DHCP leases Screen

10.3 SNMP

Figure 38. SNMP Screen displays the status of SNMP information.



Diagnostics: Logs

System | DHCP | SNMP | Settings

Last 50 SNMP log entries	
Oct 6 14:20:21	snmpd[80]: datxf:
Oct 6 14:20:21	snmpd[80]: Initializing
Oct 6 14:20:21	snmpd[80]: datxf:
Oct 6 14:20:21	snmpd[80]: Did initialize
Oct 6 14:20:24	snmpd[80]: Cannot find module (IP-MIB): At line 0 in (none)
Oct 6 14:20:24	snmpd[80]: Cannot find module (IF-MIB): At line 0 in (none)
Oct 6 14:20:24	snmpd[80]: Cannot find module (TCP-MIB): At line 0 in (none)
Oct 6 14:20:24	snmpd[80]: Cannot find module (UDP-MIB): At line 0 in (none)
Oct 6 14:20:24	snmpd[80]: Cannot find module (HOST-RESOURCES-MIB): At line 0 in (none)
Oct 6 14:20:25	snmpd[80]: Cannot find module (SNMPv2-MIB): At line 0 in (none)
Oct 6 14:20:25	snmpd[80]: Cannot find module (SNMPv2-SMI): At line 0 in (none)
Oct 6 14:20:25	snmpd[80]: Cannot find module (NOTIFICATION-LOG-MIB): At line 0 in (none)
Oct 6 14:20:25	snmpd[80]: Cannot find module (DISMAN-EVENT-MIB): At line 0 in (none)
Oct 6 14:20:25	snmpd[80]: Cannot find module (DISMAN-SCHEDULE-MIB): At line 0 in (none)

Figure 38. SNMP Screen

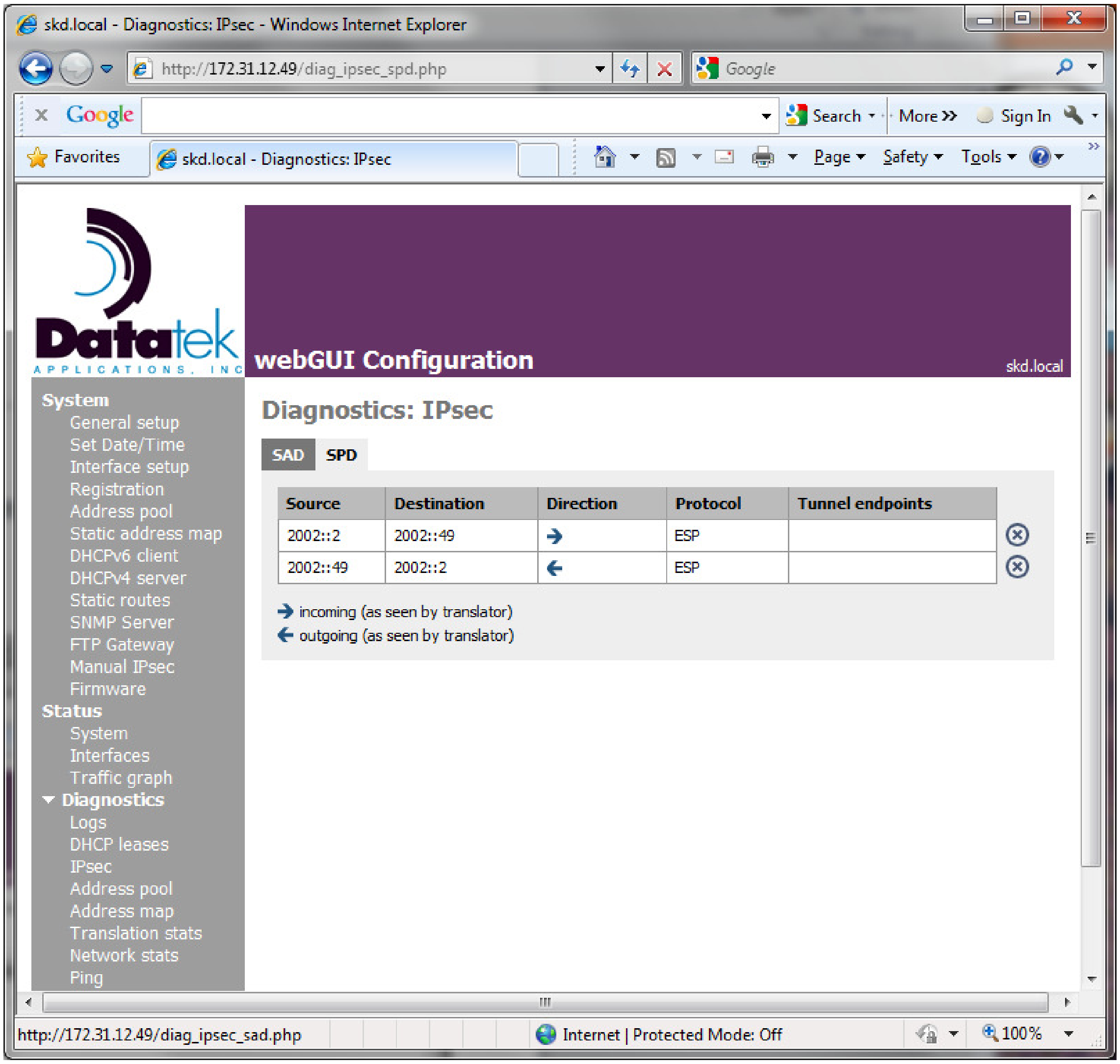
10.4 IPSec

The form below displays the Security Policies (SPs) and Security Associations (SAs) as they appear in the system.

SPD

The Security Policy Database (SPD) tab displays what type of data must be protected by IPSec as shown in **Figure 39. Security Policy Database Screen.**

Each entry has a source and destination address, direction and tunnel endpoints if the policy is for tunnel mode. The tunnel endpoints are the addresses used for the outer IPv6 packet header.



Diagnostics: IPsec

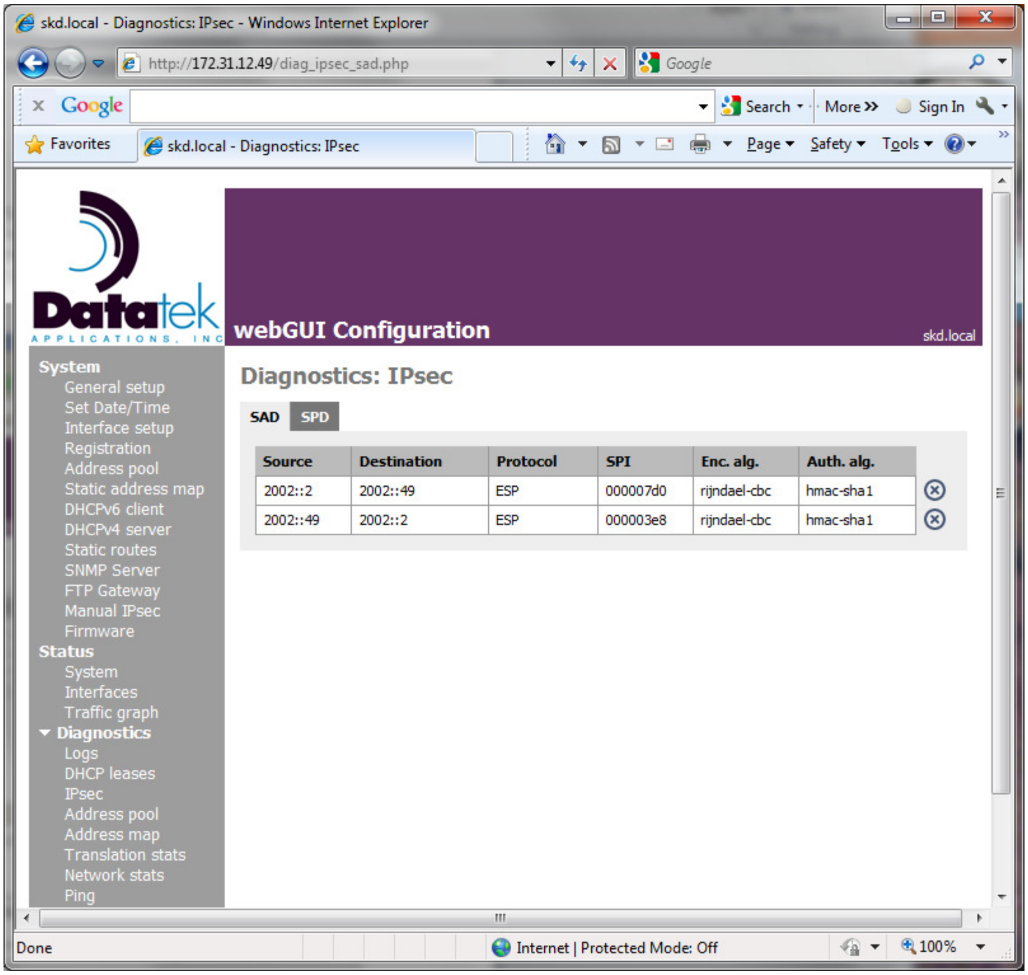
Source	Destination	Direction	Protocol	Tunnel endpoints
2002::2	2002::49	→	ESP	
2002::49	2002::2	←	ESP	

→ incoming (as seen by translator)
← outgoing (as seen by translator)

Figure 39. Security Policy Database Screen

SAD

The Security Association Database (SAD) tab displays how data that is to be protected as determined by the SPD is protected. Each entry shows the source and destination addresses, type of encryption and authentication algorithms, type of IPSec header and uniquely identifying SPI, as shown in **Figure 40. Security Association Database Screen.**



Diagnostics: IPsec

SAD SPD

Source	Destination	Protocol	SPI	Enc. alg.	Auth. alg.	
2002::2	2002::49	ESP	000007d0	rijndael-cbc	hmac-sha1	⊗
2002::49	2002::2	ESP	000003e8	rijndael-cbc	hmac-sha1	⊗

Figure 40. Security Association Database Screen

Note

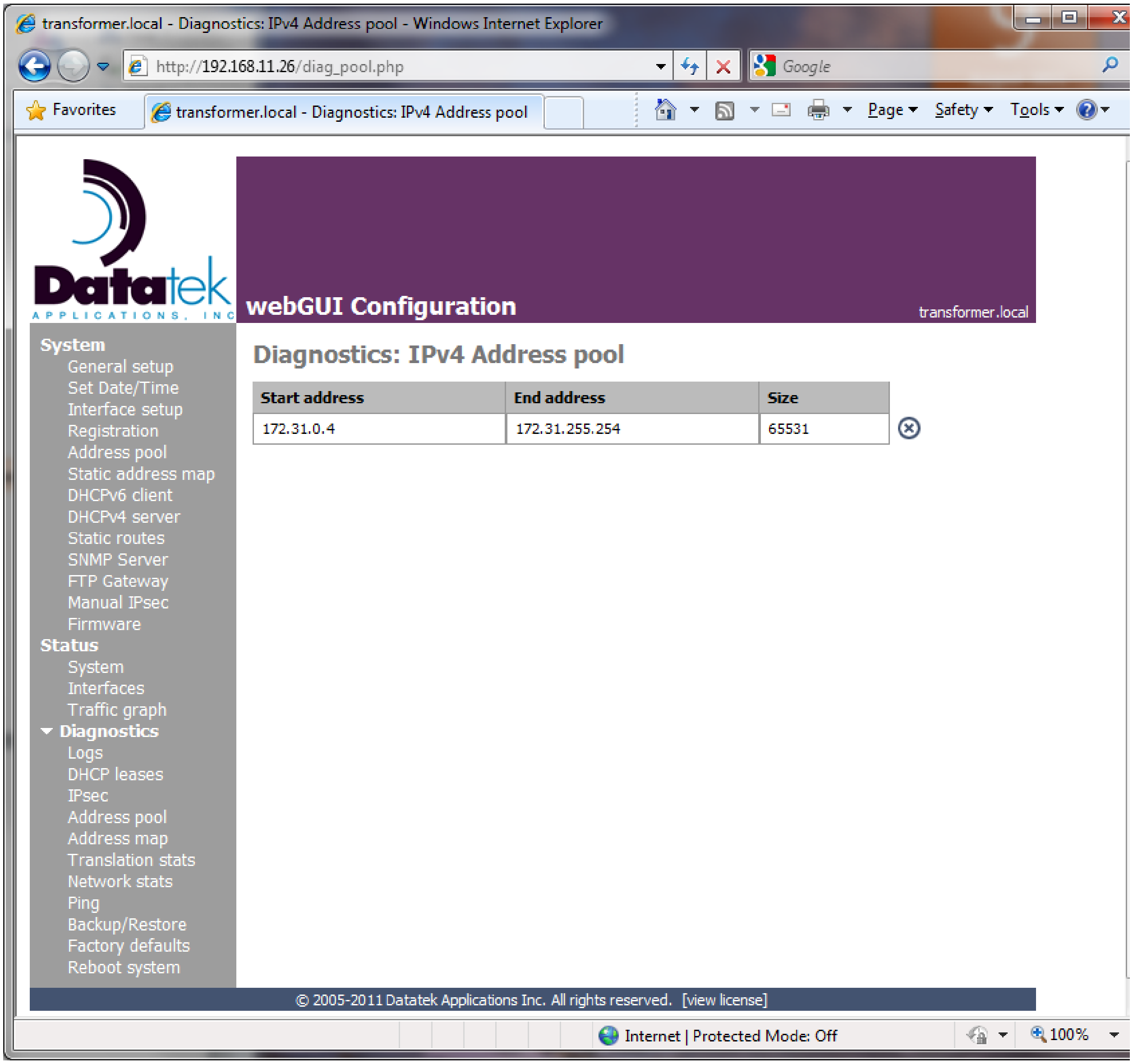
This symbol ⊗ at the end of each ***SPD or SAD entry is clicked to delete the entry.***

Warning

This is not recommended except as a means of troubleshooting. Do not delete any entries unless you know what you're doing.

10.5 Address pool

Figure 41. IPv4 Address pool Screen displays the range and size of the addresses remaining in the Transformer IPv4 address pool. It shows the starting and ending addresses still available in the pool (as opposed to configured for the pool), as well as the number of available addresses (size).



Diagnostics: IPv4 Address pool

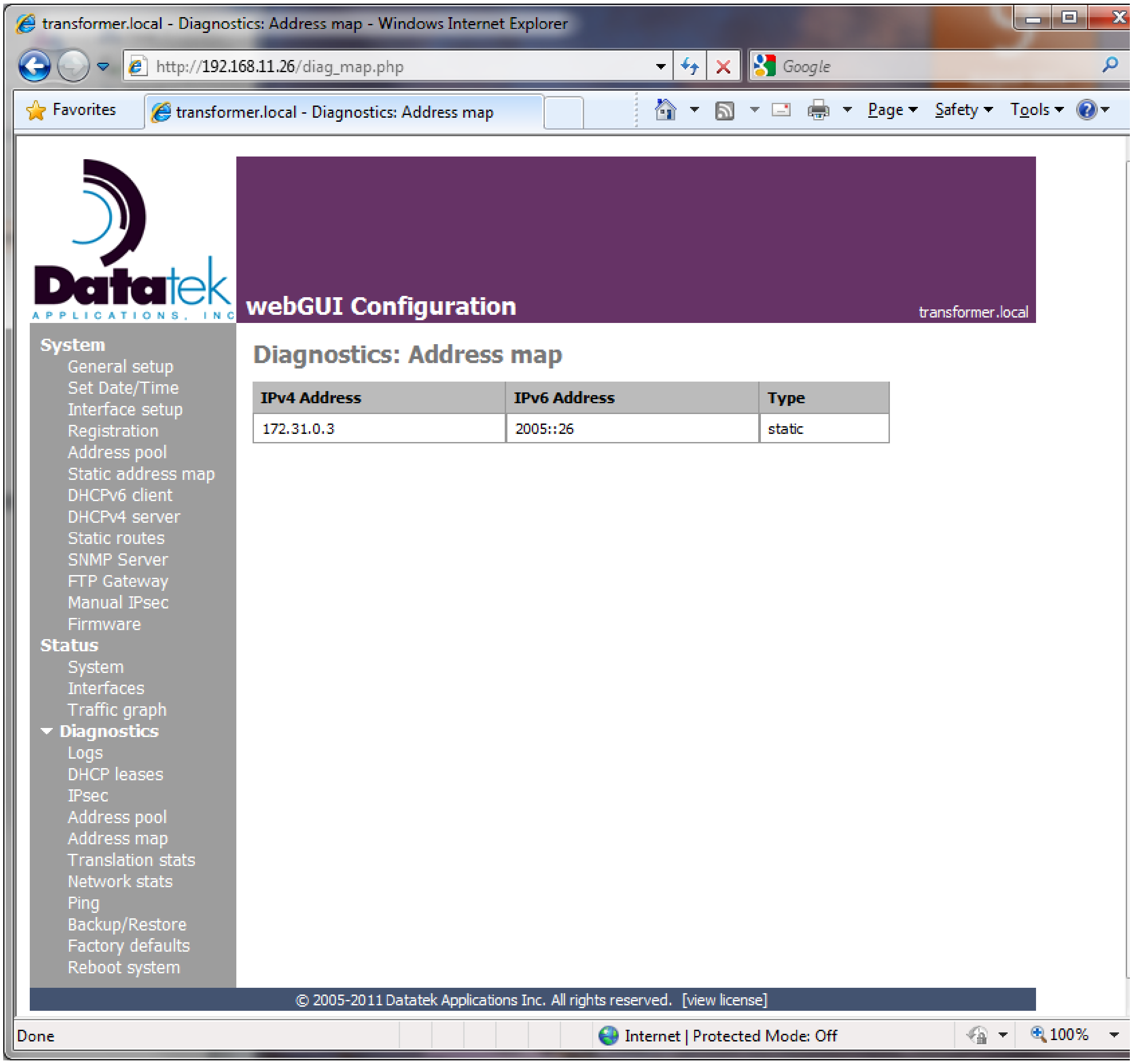
Start address	End address	Size
172.31.0.4	172.31.255.254	65531

© 2005-2011 Datatek Applications Inc. All rights reserved. [view license]

Figure 41. IPv4 Address pool Screen

10.6 Address map

Figure 42. Address map Screen displays the actual Transformer mapping table. It shows how the IPv6 and IPv4 addresses are mapped, as well as the Type, which can be acquired statically or dynamically. Both the configured static mapping and the local forward mapping will appear as 'static'.



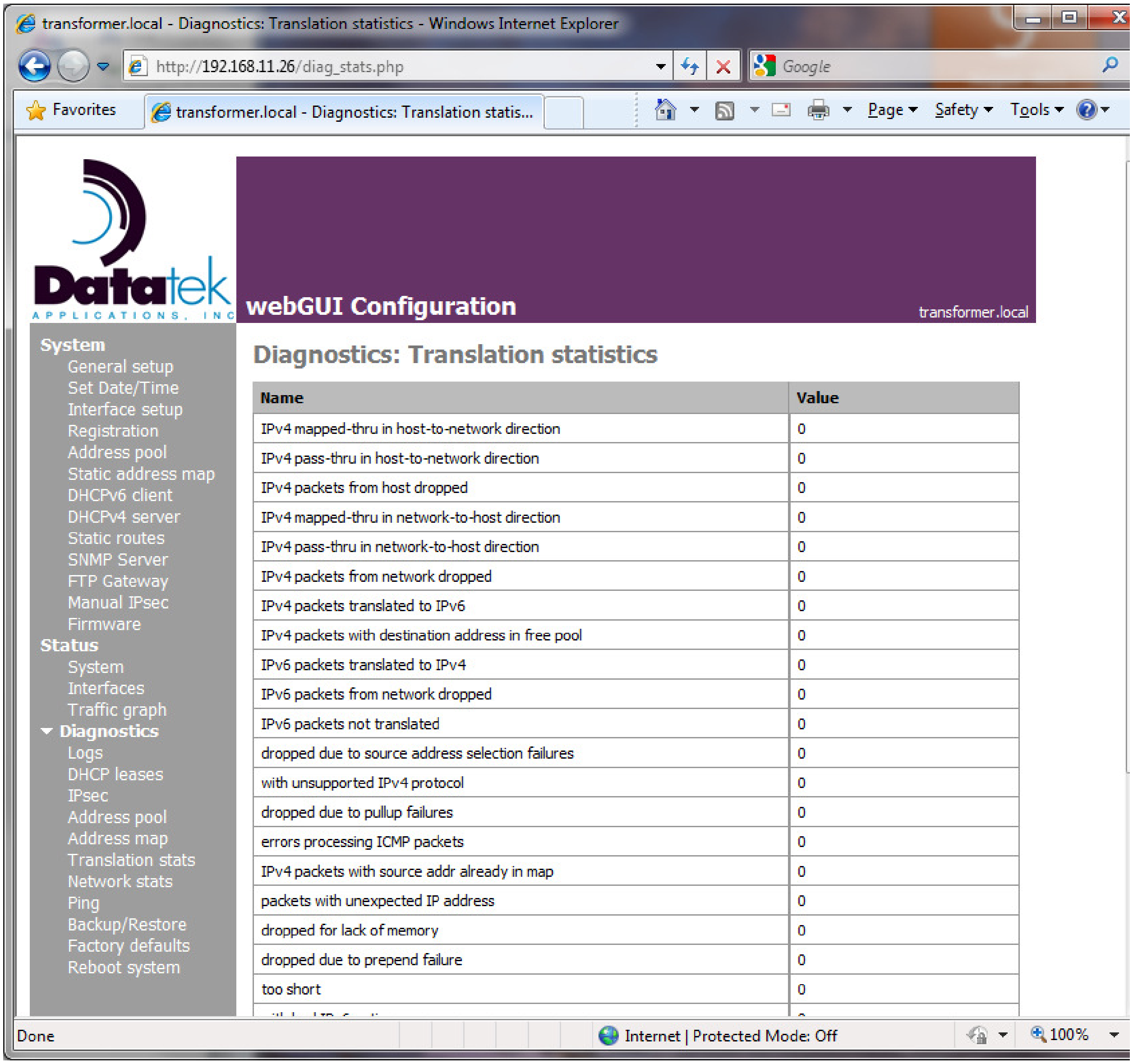
Diagnostics: Address map

IPv4 Address	IPv6 Address	Type
172.31.0.3	2005::26	static

Figure 42. Address map Screen

10.7 Translation statistics

Figure 43. Translation statistics Screen displays various Transformer statistics useful to the user.



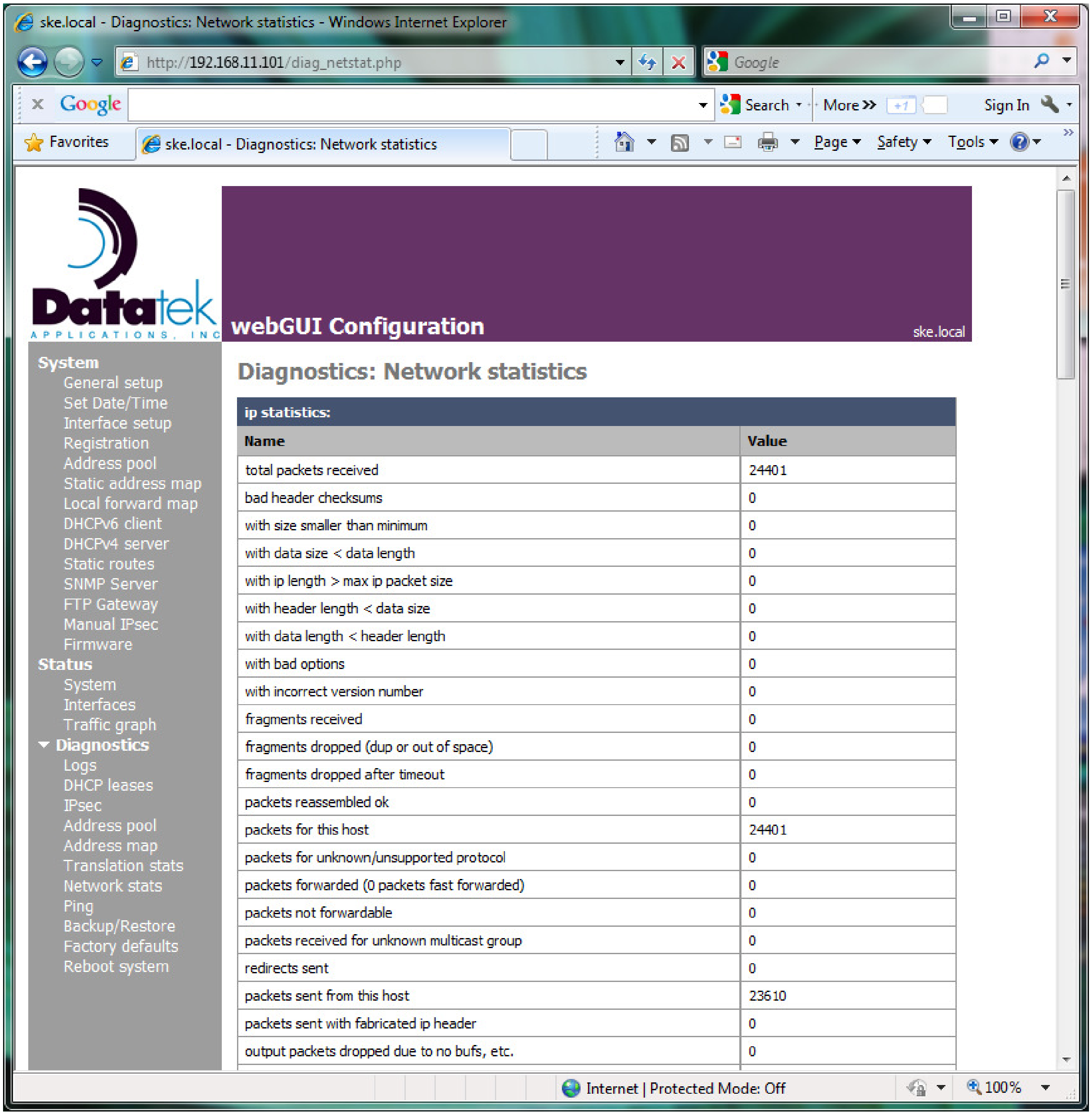
Diagnostics: Translation statistics

Name	Value
IPv4 mapped-thru in host-to-network direction	0
IPv4 pass-thru in host-to-network direction	0
IPv4 packets from host dropped	0
IPv4 mapped-thru in network-to-host direction	0
IPv4 pass-thru in network-to-host direction	0
IPv4 packets from network dropped	0
IPv4 packets translated to IPv6	0
IPv4 packets with destination address in free pool	0
IPv6 packets translated to IPv4	0
IPv6 packets from network dropped	0
IPv6 packets not translated	0
dropped due to source address selection failures	0
with unsupported IPv4 protocol	0
dropped due to pullup failures	0
errors processing ICMP packets	0
IPv4 packets with source addr already in map	0
packets with unexpected IP address	0
dropped for lack of memory	0
dropped due to prepend failure	0
too short	0

Figure 43. Translation statistics Screen

10.8 Network statistics

Figure 44. Network statistics Screen displays Network statistics of the Transformer.



Diagnostics: Network statistics

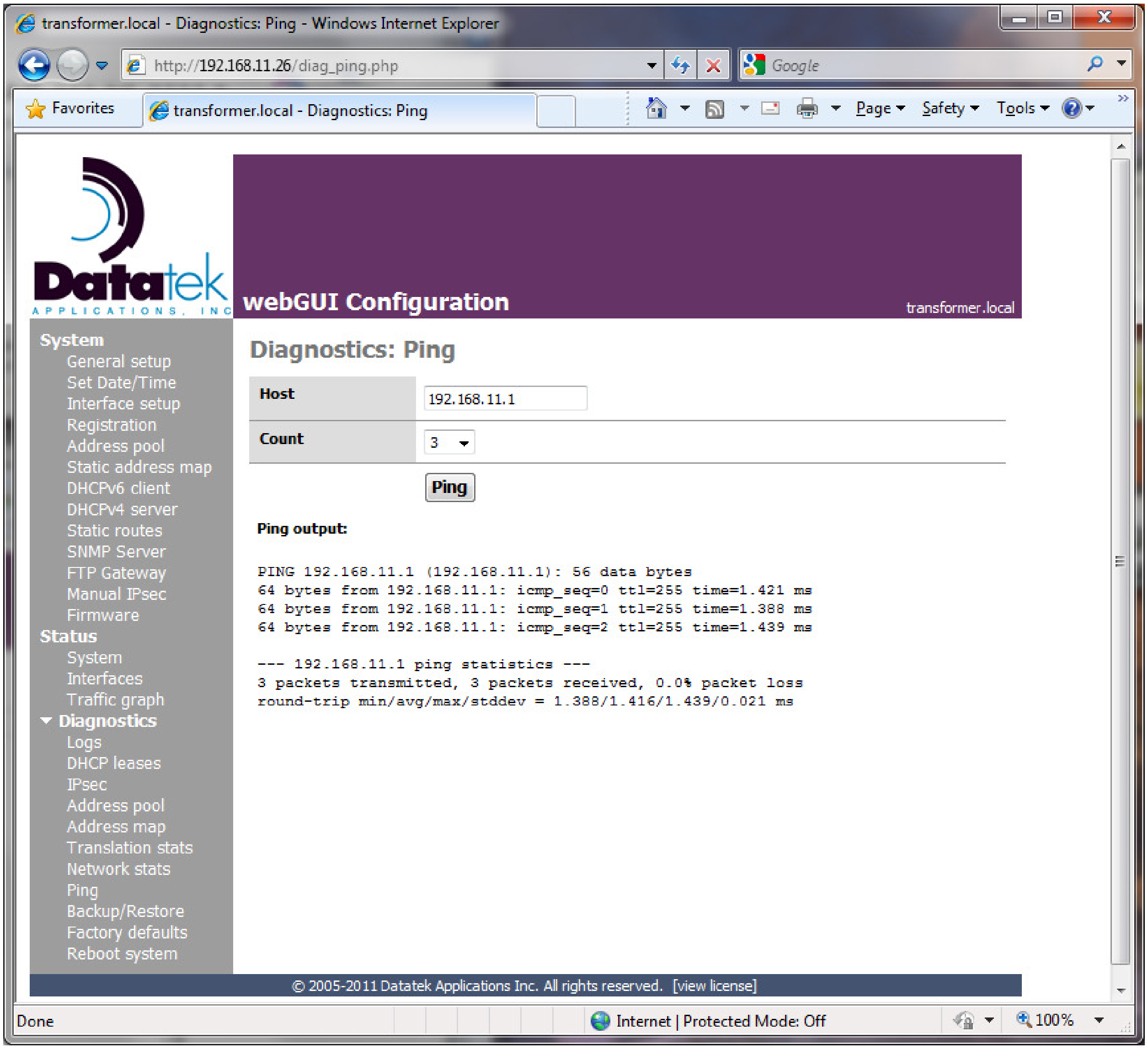
ip statistics:

Name	Value
total packets received	24401
bad header checksums	0
with size smaller than minimum	0
with data size < data length	0
with ip length > max ip packet size	0
with header length < data size	0
with data length < header length	0
with bad options	0
with incorrect version number	0
fragments received	0
fragments dropped (dup or out of space)	0
fragments dropped after timeout	0
packets reassembled ok	0
packets for this host	24401
packets for unknown/unsupported protocol	0
packets forwarded (0 packets fast forwarded)	0
packets not forwardable	0
packets received for unknown multicast group	0
redirects sent	0
packets sent from this host	23610
packets sent with fabricated ip header	0
output packets dropped due to no bufs, etc.	0

Figure 44. Network statistics Screen

10.9 Ping

The Ping form is used to test connectivity between the Transformer and a device on either the IPv6 or the IPv4 side. However, the IPv6 addresses representing the host side cannot be reached by the Transformer's ping. **Figure 45. Ping Screen** shows the results of the Ping command.



Diagnostics: Ping

Host	192.168.11.1
Count	3

Ping output:

```
PING 192.168.11.1 (192.168.11.1): 56 data bytes
64 bytes from 192.168.11.1: icmp_seq=0 ttl=255 time=1.421 ms
64 bytes from 192.168.11.1: icmp_seq=1 ttl=255 time=1.388 ms
64 bytes from 192.168.11.1: icmp_seq=2 ttl=255 time=1.439 ms

--- 192.168.11.1 ping statistics ---
3 packets transmitted, 3 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 1.388/1.416/1.439/0.021 ms
```

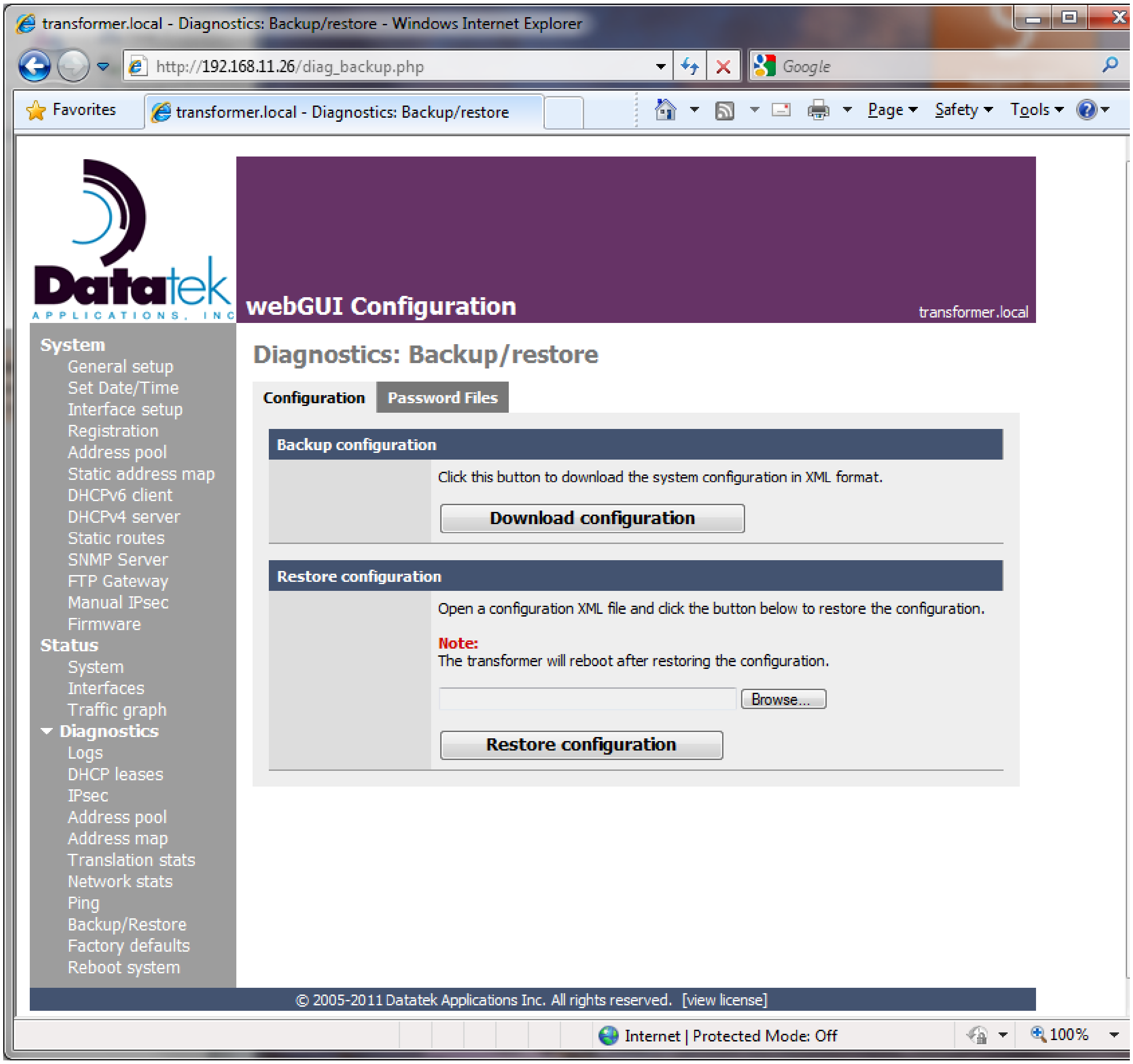
© 2005-2011 Datatek Applications Inc. All rights reserved. [view license]

Figure 45. Ping Screen

10.10 Backup/Restore

Configuration

The Configuration tab is selected to backup the system configuration to a file on the host that is running the web browser or restore the system configuration from a file on the web browser host to the Transformer. This selection will also enable you to restore a previously-saved configuration file to the Transformer. This is shown in **Figure 46. Backup/restore Configuration Screen.**



Diagnostics: Backup/restore

Backup configuration

Click this button to download the system configuration in XML format.

Restore configuration

Open a configuration XML file and click the button below to restore the configuration.

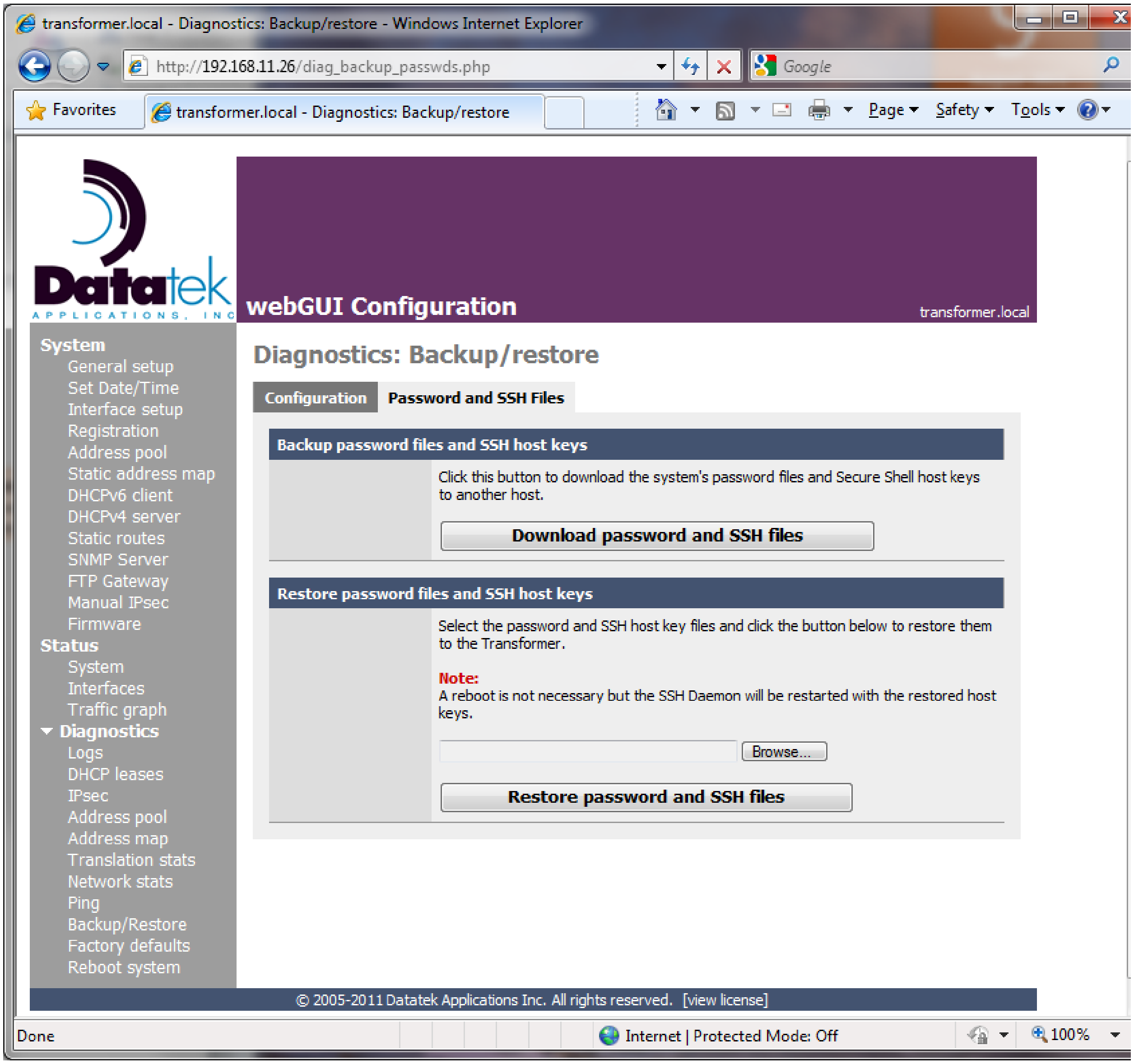
Note:
The transformer will reboot after restoring the configuration.

© 2005-2011 Datatek Applications Inc. All rights reserved. [view license]

Figure 46. Backup/restore Configuration Screen

Password and SSH Files

The Password and SSH Files tab is selected to backup the password files used by Secure Shell (SSH) to the host that is running the web browser or restore them from the web browser host to the Transformer. This is shown in **Figure 47. Backup/restore Password and SSH Files Screen**



Click this button to download the system's password files and Secure Shell host keys to another host.

Select the password and SSH host key files and click the button below to restore them to the Transformer.

Note:
A reboot is not necessary but the SSH Daemon will be restarted with the restored host keys.

© 2005-2011 Datatek Applications Inc. All rights reserved. [view license]

Figure 47. Backup/restore Password and SSH Files Screen

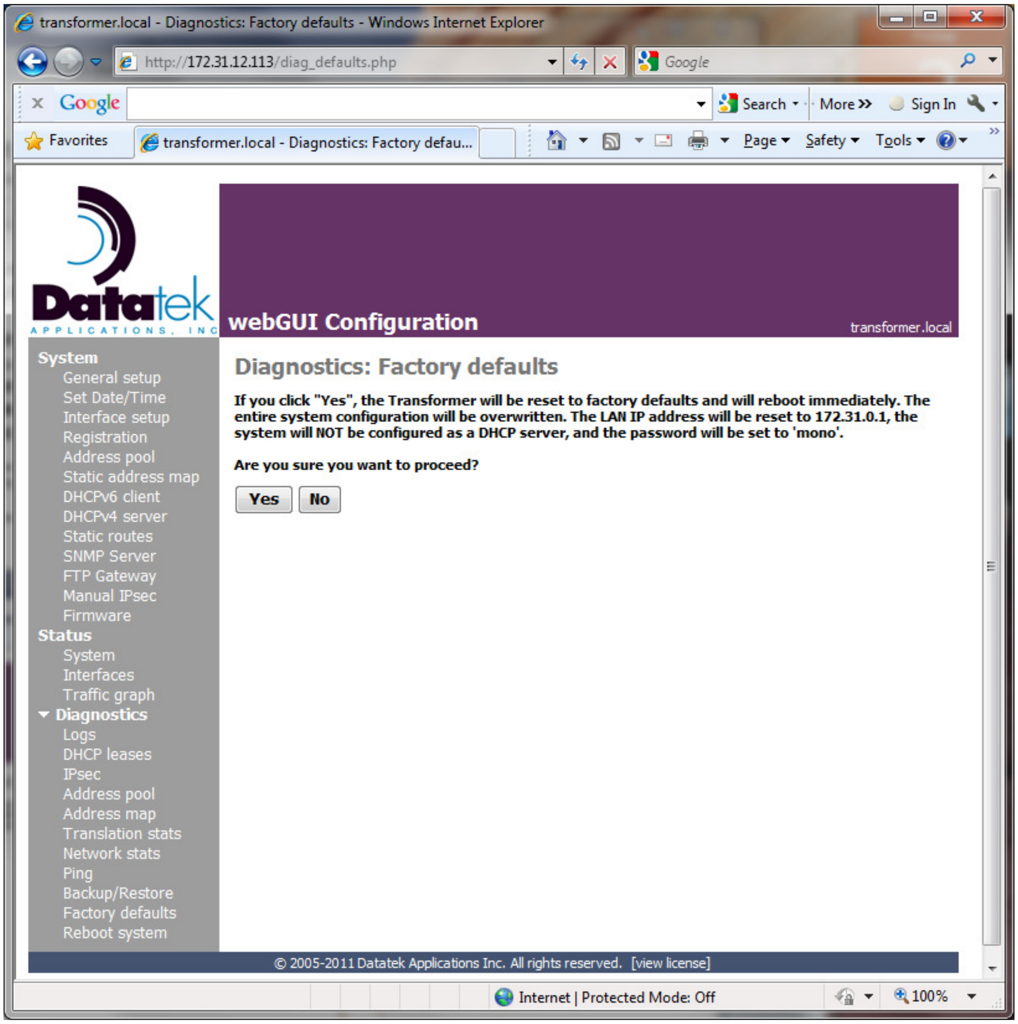
10.11 Factory defaults

The Factory defaults form provides the means to clear out the current configuration and restore it to the defaults that were shipped from the factory.

Use the Diagnostics Backup/Restore form first to save a copy of your configuration. After clearing the by responding 'Yes' to the question, 'Are you sure you want to proceed' the Transformer will automatically reboot. After rebooting, the Transformer Console Menu must be used to enter the IPv6/Host and IPv6/Network addresses necessary to access the webGUI again. **Figure 48. Factory defaults Screen** is shown below.

Warning

Setting the unit back to the factory defaults will remove the authorization code and a new one will need to be obtained from Datatek



Diagnostics: Factory defaults

If you click "Yes", the Transformer will be reset to factory defaults and will reboot immediately. The entire system configuration will be overwritten. The LAN IP address will be reset to 172.31.0.1, the system will NOT be configured as a DHCP server, and the password will be set to 'mono'.

Are you sure you want to proceed?

Figure 48. Factory defaults Screen

10.12 Reboot System

The Reboot System form is used to reboot the Transformer and apply any configuration changes made to the system. **Figure 49. Reboot System Screen** is shown below.

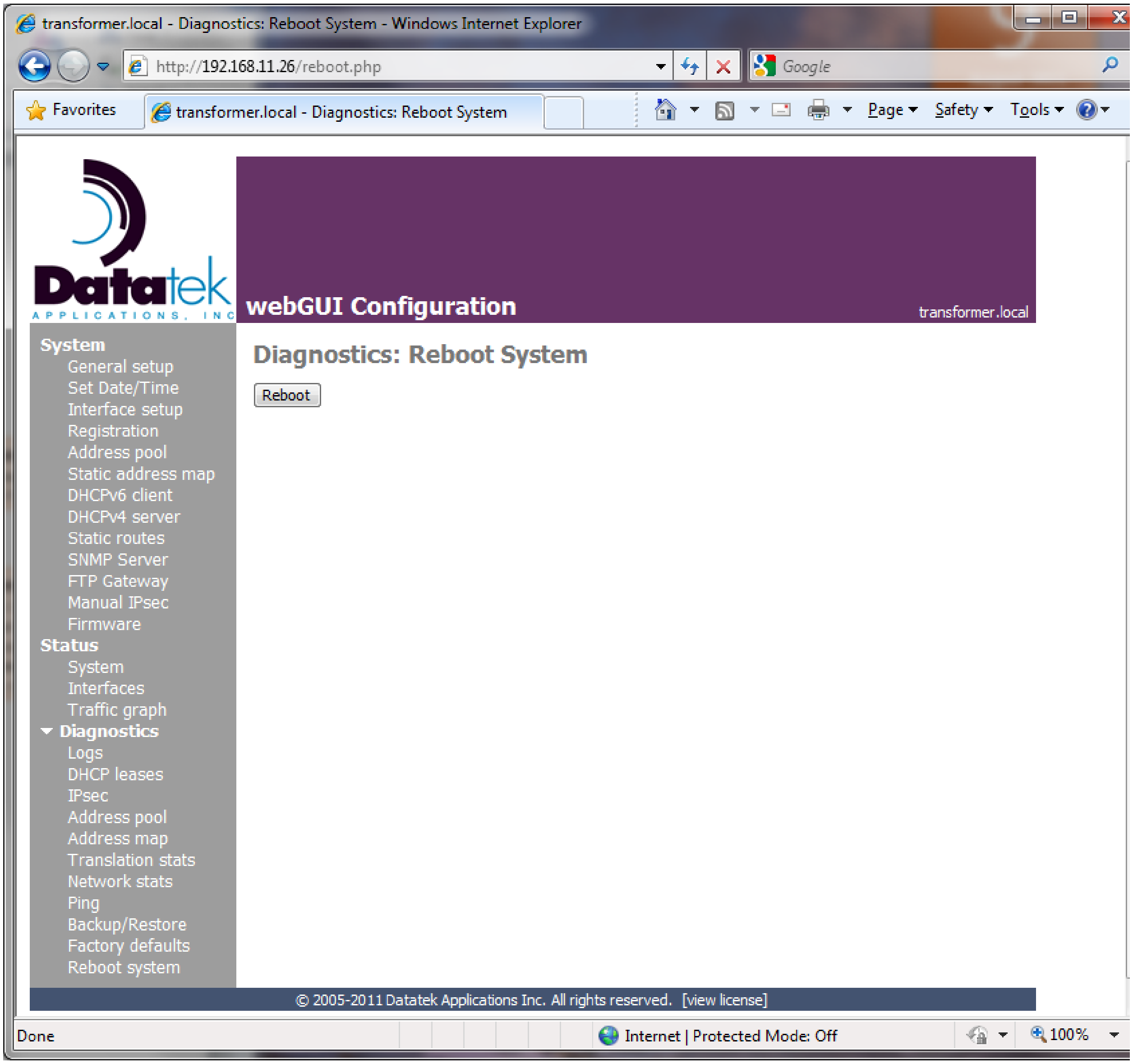


Figure 49. Reboot System Screen

11 End-User License Agreement for Datatek IPv4-IPv6 Transformer

This License Agreement "("License"") is a legal contract between you and the manufacturer ("Manufacturer") of the software product(s) you acquired identified as ("SOFTWARE"). The SOFTWARE may include printed materials that accompany the SOFTWARE. Any software provided along with the SOFTWARE that is associated with a separate end-user license agreement is licensed to you under the terms of that license agreement. By installing, copying, downloading, accessing or otherwise using the SOFTWARE, you agree to be bound by the terms of this LICENSE. If you do not agree to the terms of this LICENSE, Manufacturer is unwilling to license the SOFTWARE to you. In such event, you may not use or copy the SOFTWARE, and you should promptly contact Manufacturer for instructions on return of the unused product(s) for a refund.

Software License

You may only install and use one copy of the SOFTWARE on one computer (unless otherwise licensed by Manufacturer). Notwithstanding the foregoing and except as otherwise provided below, any number of Devices may access or otherwise utilize the services of the SOFTWARE. You may not reverse engineer, decompile, or disassemble the SOFTWARE, except and only to the extent that such activity is expressly permitted by applicable law notwithstanding this limitation. You may not rent, lease or lend the SOFTWARE in any manner. You may permanently transfer all of your rights under this LICENSE provided you retain no copies, you transfer all of the SOFTWARE (including all component parts, the media and printed materials, any upgrades, this LICENSE and, if applicable, the Certificate(s) of Authenticity), and the recipient agrees to the terms of this LICENSE. If the SOFTWARE is an upgrade, any transfer must also include all prior versions of the SOFTWARE. Without prejudice to any other rights, Manufacturer may terminate this LICENSE if you fail to comply with the terms and conditions of this LICENSE. In such event, you must destroy all copies of the SOFTWARE and all of its component parts.

Intellectual Property Rights

The SOFTWARE is licensed, not sold to you. The SOFTWARE is protected by copyright laws and international copyright treaties, as well as other intellectual property laws and treaties. You may not copy the printed materials accompanying the SOFTWARE. All title and intellectual property rights in and to the content which may be accessed through use of the SOFTWARE is the property of the respective content owner and may be protected by applicable copyright or other intellectual property laws and treaties. This LICENSE grants you no rights to use such content. All rights not expressly granted under this LICENSE are reserved Manufacturer and its licensors (if any).

Software Support

SOFTWARE support is provided by Manufacturer, or its affiliates or subsidiaries separate from the computer on which it may be installed. SOFTWARE support is limited to the warranty period stated below unless either a separate maintenance contract has been consummated between you and the manufacturer or the manufacturer has agreed in writing at the time of purchase by you of the software to an extension of the warranty. Should you have any questions concerning this LICENSE, or if you desire to contact Manufacturer for any other reason, please refer to the address provided in the documentation for the SOFTWARE.

Export Restrictions

You agree that you will not export or re-export the SOFTWARE to any country, person, or entity subject to U.S. export restrictions. You specifically agree not to export or re-export the SOFTWARE: (i) to any country to which the U.S. has embargoed or restricted the export of goods or services, which as of March 1998 include, but are not necessarily limited to Cuba, Iran, Iraq, Libya, North Korea, Sudan and Syria, or to any national of any such country, wherever located, who intends to transmit or transport the products back to such country; (ii) to any person or entity who you know or have reason to know will utilize the SOFTWARE or portion thereof in the design, development or production of nuclear, chemical or biological weapons; or (iii) to any person or entity who has been prohibited from participating in U.S. export transactions by any federal agency of the U.S. government.

Limited Warranty

Manufacturer warrants that (a) the SOFTWARE will perform substantially in accordance with the accompanying written materials for a period of ninety (90) days from the date of shipment from Datatek Applications, Inc. Software support is limited to the hours of 9 AM to 5 PM ET Monday through Friday excluding Datatek Applications observed holidays. Other coverage and extended warranty may be purchased at additional cost. Any implied warranties on the SOFTWARE are limited to ninety (90) days. Some states/jurisdictions do not allow limitations on duration of an implied warranty, so the above limitation may not apply to you.

Manufacturer's and its suppliers' entire liability and your exclusive remedy shall be, at Manufacturer's option, either (a) return of the price paid, or (b) repair or replacement of the SOFTWARE that does not meet this Limited Warranty and which is returned to Manufacturer with a copy of your receipt. This Limited Warranty is void if failure of the SOFTWARE has resulted from accident, abuse, or misapplication. Any replacement SOFTWARE will be warranted for the remainder of the original warranty period or thirty (30) days, whichever is longer.

No Other Warranties

To the maximum extent permitted by applicable law, manufacturer and its suppliers disclaim all other warranties, either express or implied, including, but not limited to implied warranties of merchantability, fitness for a particular purpose and non-infringement, with regard to the software and the accompanying written materials. This limited warranty gives you specific legal rights. You may have others, which vary from state/jurisdiction to state/jurisdiction.

Special Provisions

The SOFTWARE and documentation are provided with RESTRICTED RIGHTS. Use, duplication, or disclosure by the United States Government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Software clause at DFARS 252.227-7013 or subparagraphs (c)(1) and (2) of the Commercial Software-Restricted Rights at 48 CFR 52.227-19, as applicable. Manufacturer is Datatek Applications, Inc., 379 Campus Drive, Somerset, NJ 08873.

If you acquired the SOFTWARE in the United States of America, this Software License is governed by the laws of the State of New Jersey, excluding its choice of laws provisions. If you acquired the SOFTWARE outside the United States of America, local law may apply. This LICENSE constitutes the entire understanding and agreement between you and the Manufacturer in relation to the SOFTWARE and supersedes any and all prior or other communications, statements, documents, agreements or other information between the parties with respect to the subject matter hereof.

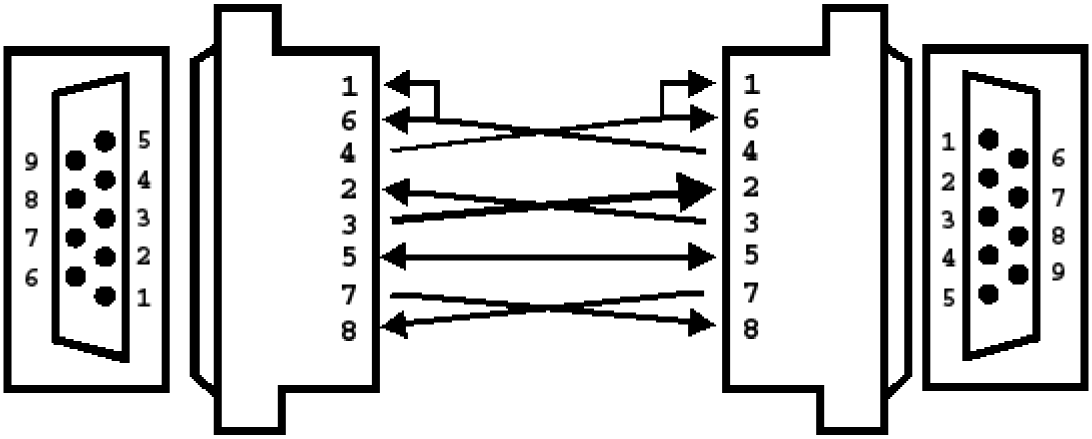
Limitation of Liability

To the maximum extent permitted by applicable law, in no event shall Manufacturer or its suppliers be liable for any damages whatsoever (including without limitation, special, incidental, consequential, or indirect damages for personal injury, loss of business profits, business interruption, loss of business information, or any other pecuniary loss) arising out of the use of or inability to use this product, even if Manufacturer has been advised of the possibility of such damages. In any case, Manufacturer’s and its suppliers’ entire liability under any provision of this License shall be limited to the amount actually paid by you for the SOFTWARE. Because some states/jurisdictions do not allow the exclusion or limitation of liability for consequential or incidental damages, the above limitation may not apply to you.

Appendix A

9-Pin Null Modem Connector Pinouts

DB9 Pin Layout
Pin 1 - Carrier Detect (CD) Pin 2 - Receive Data (RD) Pin 3 - Transmit Data (TD) Pin 4 - Data Terminal Ready (DTR) Pin 5 – Ground (GND) Pin 6 - Data Set Ready (DSR) Pin 7 - Ready To Send (RTS) Pin 8 - Clear To Send (CTS) Pin 9 - Ring Indicator (RI)



Appendix B

Specifications

Physical

Flash Memory: 4GB

Power Supply: 7-20V Internal DC Power

LAN Ports: Two 10/100Mbps Ethernet; RJ-45

USB Ports: Two USB 2.0

Console: One DB9 Serial Male Port

Buttons: System Reset/Factory Network Reset

LEDs: Unit Power, Booting, LAN Link/Activity

OS: FreeBSD 8.0

Mean Time Between Failures (MTBF): Calculated 100,000+ hours

Power Consumption: 4W typical, 6W peak

Form Factor: 1U desktop design

Environmental

Dimensions: (W x H x D) 6.25 in. x 1.0 in x 6.25 in. (159mm x 25mm x 159mm)

Unit Weight: 1.0 lb (0.45 kg)

Power: External adaptor - 100-120VAC, 50/60Hz (US plug style)

Cooling: None - Fanless

Operating temperature: 32-122 degrees F (0-50 degrees C)

Certification: FCC Part 15, CE EN61000-6-3, CE EN61000-6-2

Safety: UL Safety and Environmental Compliance